## Li(p)-service? An algorithm for computing p-adic polylogarithms

Besser, A.; de Jeu, R.M.H.

***published in***
Mathematics of computation
2008

***DOI (link to publisher)***
10.1090/s0025-5718-07-02027-3

***document version***
Publisher's PDF, also known as Version of record

MATHEMATICS OF COMPUTATION
Volume 77, Number 262, April 2008, Pages 1105–1134
S 0025-5718(07)02027-3
Article electronically published on November 5, 2007

# $\mathbf{Li}^{(p)}$-SERVICE? AN ALGORITHM FOR COMPUTING $p$-ADIC POLYLOGARITHMS

AMNON BESSER AND ROB DE JEU

Abstract. We describe an algorithm for computing Coleman's $p$-adic polylogarithms up to a given precision.

## 1. Introduction

It is well known that, for a number field $k$ with ring of integers $\mathcal{O}_k$, there is a relation between the regulator of the group of units of $\mathcal{O}_k$, $\mathcal{O}_k^*$, and the residue of $\zeta_k(s)$ at $s = 1$. In terms of $K$-theory, $\mathcal{O}_k^* \cong K_1(\mathcal{O}_k)$, and Borel in [6] showed that this relation generalizes, for $n = 2, 3, \ldots$, to a similar relation between a suitably defined regulator of the higher $K$-group $K_{2n-1}(\mathcal{O}_k)$ and the value of $\zeta_k(s)$ at $s = n$.

However, it is far more difficult to find explicit non-trivial elements in those higher $K$-groups than in $\mathcal{O}_k^*$. But $K_{2n-1}(\mathcal{O}_k) \cong K_{2n-1}(k)$ for $n \geq 2$ and Zagier in [17] gave a conjectural description of the latter groups tensored with $\mathbb{Q}$. His construction always gives a $\mathbb{Q}$-subspace (see, e.g., [9]), and gives the whole of $K_3(k) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $K_5(k) \otimes_{\mathbb{Z}} \mathbb{Q}$ for all number fields $k$, as well as of $K_{2n-1}(k) \otimes_{\mathbb{Z}} \mathbb{Q}$ for all $n \geq 2$ if $k$ is cyclotomic (see loc. cit. where this is deduced from results by Suslin, Goncharov and Zagier respectively).

The regulator for $\mathcal{O}_k^*$ is defined as the determinant of a matrix with its entries the logarithm of the absolute value of certain elements of $\mathcal{O}_k^*$ embedded into $\mathbb{C}$. In Zagier's conjecture the Borel regulator for $K_{2n-1}(k) \cong K_{2n-1}(\mathcal{O}_k)$ is obtained as the determinant of a matrix with its entries suitable $\mathbb{Q}$-linear combinations of the values at certain elements of $k$ embedded into $\mathbb{C}$ of the $n$-th (real) polylogarithm.

This $n$-th real polylogarithm is obtained from the complex polylogarithm $\mathrm{Li}_n(z)$, which is defined by the power series

$$\mathrm{Li}_n(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^n} \qquad (n \geq 1) \tag{1.1}$$

on the open unit disc in $\mathbb{C}$. It can be continued analytically to a multi-valued function on $\mathbb{C} \setminus \{0, 1\}$. The real-valued modification is easily computed from this. For the numerical verification of the conjectures in the context of Zagier's conjecture, it is important to have an efficient implementation of the complex polylogarithm, as in, for example, PARI-GP.

Received by the editor June 19, 2006 and, in revised form, December 18, 2006.
2000 *Mathematics Subject Classification.* Primary 11Y16, 11G55; Secondary 11S80.
*Key words and phrases.* Computational number theory, Coleman integration, $p$-adic polylogarithm.

There is a conjectural $p$-adic analogue of Borel's theorem which fits into the general context of relations between regulators of $K$-groups and special values of $L$-functions as conjectured by Beilinson (see [1] or [13]). Its predictions are rather similar, but somewhat more involved, using the syntomic regulator [2] rather than the Beilinson regulator. In the case of totally real number fields it follows from [5] that the $p$-adic regulator on the part of the $K$-groups given by Zagier's conjecture[1] is given by a determinant as before, but with the complex polylogarithm replaced with the *$p$-adic polylogarithm*.

The $p$-adic polylogarithm is an analogue of its complex cousin. It was defined by Coleman [7] using the technique now referred to as *Coleman integration*. On the open unit disc in $\mathbb{C}_p$, the so called field of $p$-adic complex numbers, it is again defined by the power series (1.1). To extend it to a function defined on $\mathbb{C}_p \setminus \{1\}$ Coleman uses a technique he called "analytic continuation along Frobenius", which is rather involved. As a consequence, it is not so easy to compute the functions defined in this way. To our knowledge there has been only one attempt to compute Coleman integrals in the literature [8], with very limited precision.

Recently we embarked on a project of testing numerically the $p$-adic analogue of Borel's theorem (see [4]). This requires the computation of $p$-adic $L$-functions and $p$-adic polylogarithms up to a given precision. The present work is concerned with an algorithm for the latter. In the process of describing the set-up for the algorithm we obtain bounds for $|\mathrm{Li}_n(\zeta)|$ for a root of unity $\zeta$ of order not a power of $p$ that may be of independent interest (see the end of Section 4).

**Acknowledgments.** The second author would like to thank the Newton Institute for a productive stay during the autumn of 2002, during which this paper germinated and a first version of an implementation of the algorithm was written. He would also like to thank the University of Alberta and the Tata Institute of Fundamental Research for very productive visits, and the EC network Arithmetic Algebraic Geometry for travel support. He is grateful to Nils Bruin for sharing his magic in order to overcome some aspects of programming in MAGMA and to Karim Belabas for his comments on the last section of the paper and the implementation of the algorithm. Finally, both authors would like to thank the referee for making various suggestions for improving the paper.

## 2. The $p$-adic polylogarithm

A precise definition of Coleman integration is beyond the scope of the present paper. Fortunately, in the case of $p$-adic polylogarithms there is a certain simplification that is sufficient for the computations that we give here.

Let $p$ be a prime. Recall that the field of $p$-adic complex numbers, $\mathbb{C}_p$, is the completion of the algebraic closure of the field of $p$-adic numbers $\mathbb{Q}_p$. We let $|\cdot|$ be the absolute value on $\mathbb{C}_p$, normalized such that $|p| = p^{-1}$. It corresponds to the valuation $v_p$ normalized by $v_p(p) = 1$. The residue field of $\mathbb{C}_p$ is the algebraic closure of the field with $p$ elements, $\overline{\mathbb{F}}_p$.

We consider the projective line $X = \mathbb{P}^1(\mathbb{C}_p)$. A standard open disc in $X$ with centre $a$ in $\mathbb{C}_p$ and radius $r$ is the subset $D(a,r) = \{z \in X \,|\, |z-a| < r\}$. A standard annulus with centre $a$ in $\mathbb{C}_p$ is a subset of the form $A(a,s,r) = \{z \in X \,|\, s <$

[1] There is a technical condition, satisfied for almost all primes, that we ignore here for the sake of exposition. See the introduction of [5], in particular Theorem 1.10.

$|z-a|<r\}$. Rigid analytic functions on $D(a,r)$ are power series $\sum_{i=0}^{\infty} b_i(z-a)^i$ that converge on $D(a,r)$, and rigid analytic functions on $A(a,s,r)$ are Laurent series $\sum_{i=-\infty}^{\infty} b_i(z-a)^i$ that converge on $A(a,s,r)$. For $a=\infty$ we take $D(\infty,r)=\{z\in\mathbb{C}_p\,|\,|z|>1/r\}\cup\{\infty\}$, and rigid analytic functions on it are power series in $1/z$ that converge on $D(\infty,r)$. Similarly, $A(\infty,s,r)=\{z\in\mathbb{C}_p\,|\,1/s>|z|>1/r\}$, and rigid analytic functions on it are Laurent series in $1/z$ that converge on $A(\infty,s,r)$.

**Definition 2.1.** A branch of the $p$-adic logarithm is a group homomorphism

$$\log:\mathbb{C}_p^*\to\mathbb{C}_p$$

given by the usual power series $\log(1+z)=z-z^2/2+z^3/3-\cdots$ when $|z|<1$.

*Remark* 2.2. A branch of the $p$-adic logarithm is determined by specifying $\log(p)$ in $\mathbb{C}_p$, as follows. If $v_p(z)=0$, then $z$ reduces to an element of $\overline{\mathbb{F}}_p^*$ and therefore $z^n$ reduces to 1 for some positive $n$. Then $\log(z^n)$ is independent of the branch as it is determined by the power series given above, and $\log(z)=\log(z^n)/n$, independent of $n$. In general, if $bv_p(z)=a$ for integers $a$ and $b$ with $b$ positive, then $v_p(z^b/p^a)=0$ and $\log(z)=a\log(p)/b+\log(z^b/p^a)/b$, independent of the choice of $a$ and $b$.

We now once and for all fix a branch of the $p$-adic logarithm. All constructions that follow do depend on this choice in principle. (For the precise dependence of the functions $\mathrm{Li}_n(z)$ that we are about to describe on the choice of the branch of the logarithm, we refer to Remark 7.4 or [5, Proposition 2.6].)

We define log-type functions on $A(a,s,r)$ to be polynomials $\sum f_i\cdot(\log(z-a))^i$ with respect to $\log(z-a)$ if $a\neq\infty$ and polynomials $\sum f_i\cdot(\log z)^i$ with respect to $\log z$ if $a=\infty$, with the $f_i$ rigid analytic functions on $A(a,s,r)$. We let $\mathcal{O}_{\log}(U)$ denote the space of rigid analytic functions on $U$ if $U=D(a,r)$, and the space of log-type functions on $U$ if $U=A(a,s,r)$. We differentiate functions formally, with the rule that the derivative of $\log(z-a)$ is $1/(z-a)$. It is a basic fact, and rather easy to prove, that differentiation gives a surjective map from $\mathcal{O}_{\log}(U)$ to itself, with kernel consisting of the constants.

Consider now the system of differential equations

$$\begin{aligned}\mathrm{dLi}_1(z)&=\frac{\mathrm{d}z}{1-z},\\ \mathrm{dLi}_{n+1}(z)&=\mathrm{Li}_n(z)\frac{\mathrm{d}z}{z}\quad(n\geq 1)\end{aligned}\tag{2.3}$$

or, equivalently,

$$\begin{aligned}\mathrm{Li}_0(z)&=\frac{z}{1-z},\\ \mathrm{dLi}_{n+1}(z)&=\mathrm{Li}_n(z)\frac{\mathrm{d}z}{z}\quad(n\geq 0)\,.\end{aligned}\tag{2.4}$$

The complex polylogarithms are defined by the same system. It has singularities at 0, 1 and $\infty$. It follows from the properties of the rings $\mathcal{O}_{\log}(U)$ discussed before that on each disc or annulus $U$ not containing 0, 1 or $\infty$, (2.3) or (2.4) can be solved with $\mathrm{Li}_n(z)$ in $\mathcal{O}_{\log}(U)$. In fact, such solutions on $U$ are unique up to adding

$$c_{n-1}+\frac{c_{n-2}}{1!}\log z+\cdots+\frac{c_0}{(n-1)!}\log^{n-1}z$$

with $c_j$ in $\mathbb{C}_p$ corresponding to the constant of integration in (2.4) for $n=j$.

In particular, all such solutions are rigid analytic for all but three "residue discs" $U_a$, consisting of those points in $\mathbb{P}^1(\mathbb{C}_p)$ reducing to the same point as $a$. The three residue discs for which this does not hold a priori are $U_0$, $U_1$ and $U_\infty$. On $U_0$ it is well known (and immediate) that the series in (1.1) for $z$ in $\mathbb{C}_p$ with $|z| < 1$ and $n \geq 0$ satisfy the systems (2.3) and (2.4), and we shall in fact assume that the $\mathrm{Li}_n(z)$ on $U_0$ are given by those series. But on $U_a$ with $a = 1$ or $\infty$ the $\mathrm{Li}_n(z)$ only belong to $\mathcal{O}_{\log}(U)$ for $U = U_a \setminus \{a\}$.

Clearly, what has been said so far does not suffice to determine $\mathrm{Li}_n(z)$ uniquely. The real magic of Coleman's theory is that there is a canonical way of choosing solutions to differential equations such as in (2.3) (in general, unipotent differential equations) using a principle known as *Frobenius equivariance*. As we mentioned before, a general discussion of Coleman's theory is beyond the scope of the present work, but we explain what it means in the present context.

For this we also need the functions

$$\mathrm{Li}_n^{(p)}(z) = \mathrm{Li}_n(z) - \frac{1}{p^n}\mathrm{Li}_n(z^p)\,, \tag{2.5}$$

a priori defined for $z$ in $\mathbb{C}_p$ with $z^p \neq 1$. They satisfy conditions similar to (2.4), namely

$$\begin{aligned} \mathrm{Li}_0^{(p)}(z) &= \frac{z}{1-z} - \frac{z^p}{1-z^p}, \\ \mathrm{dLi}_{n+1}^{(p)}(z) &= \mathrm{Li}_n^{(p)}(z)\frac{\mathrm{d}z}{z} \quad (n \geq 0)\,. \end{aligned} \tag{2.6}$$

**Theorem 2.7** (Coleman)**.** *For any branch of the p-adic logarithm there exists a unique sequence of functions*

$$\mathrm{Li}_n : \mathbb{P}^1(\mathbb{C}_p) \setminus \{1, \infty\} \to \mathbb{C}_p \qquad (n \geq 0)$$

*with the properties:*

1. *the restrictions of the* $\mathrm{Li}_n$ *to every residue disc* $U = U_a$ *other than* $U_1$ *and* $U_\infty$*, and to the annuli* $U = U_1 \setminus \{1\}$ *and* $U = U_\infty \setminus \{\infty\}$*, belong to* $\mathcal{O}_{\log}(U)$ *and satisfy* (2.4)*;*
2. *the restrictions of the* $\mathrm{Li}_n$ *to* $U_0$ *are given by the series* (1.1)*;*
3. *for each* $n \geq 0$ *the function* $\mathrm{Li}_n^{(p)}(z)$ *with* $\mathrm{Li}_n^{(p)}(\infty) = 0$ *extends to a function on* $\mathbb{P}^1(\mathbb{C}_p) \setminus \{z \text{ in } \mathbb{C}_p \text{ with } z^p = 1\}$ *that on the set*

$$\mathbb{P}^1(\mathbb{C}_p) \setminus \{z \text{ in } \mathbb{C}_p \text{ with } |z-1| \leq p^{-1/(p-1)}\} \tag{2.8}$$

*is given by a convergent power series in* $1/(1-z)$*.*

*Moreover,* $\mathrm{Li}_n^{(p)}(z)$ *on the set in* (2.8) *is independent of the branch of the logarithm.*

*Proof.* We use [7]. The $\mathrm{Li}_n(z)$ are defined there in section VI (page 195) exactly to satisfy (2.4) (the definition of $\mathrm{Li}_0(z)$ in loc. cit. is incorrect) as well as $\lim_{z\to 0}\mathrm{Li}_n(z) = 0$. The fact that the polylogarithms belong to $\mathcal{O}_{\log}(U)$ for all residue discs but $U_0$ is part of the properties of Coleman integration. Using induction on $n$ it follows directly from the definition that $\mathrm{Li}_n(z)$ on $U_0$ is given by (1.1), hence lies in $\mathcal{O}_{\log}(U_0)$. The power series expansion of $\mathrm{Li}_n^{(p)}(z)$ in (3) is Proposition 6.2 of loc. cit.

As for uniqueness, we first notice that the power series expansion of $\mathrm{Li}_n^{(p)}(z)$ with respect to $1/(1-z)$ on the set in (2.8) is uniquely determined by (2.6) and its value at $\infty$ (cf. Proposition 4.3 below). In particular, $\mathrm{Li}_n^{(p)}(z)$ on this set is independent

of the branch of the logarithm. Assuming that, on each residue disc $U$, $\mathrm{Li}_{n-1}(z)$ in $\mathcal{O}_{\log}(U)$ has already been determined, the differential equation in (2.4) determines $\mathrm{Li}_n(z)$ up to a constant. Therefore $\mathrm{Li}_n(z)$ is determined up to adding a function $C(z)$ that is constant on each $U$. Since the set in (2.8) intersects every $U$ we have that $C(z) - C(z^p)/p^n = 0$. Because $z$ and $z^{p^f}$ lie in the same residue disc for some $f > 0$ this implies that $C$ is the zero function. □

*Remark* 2.9. (1) The characterisation of $\mathrm{Li}_n(z)$ in Coleman's theory is different, and requires the full force of this theory to explain.

(2) The part of $\mathbb{P}^1(\mathbb{C}_p)$ that has to be removed in part (3) of Theorem 2.7 is the disc around 1 that contains all the singularities of the differential equation satisfied by $\mathrm{Li}_n^{(p)}(z)$ except for 0 and $\infty$, i.e., the $p$-th roots of unity. The convergence of the power series in $1/(1-z)$ on the indicated domain implies a growth condition on its coefficients. We will in fact deduce, by explicit computation, a more precise growth condition on these coefficients (see Proposition 6.1).

(3) In Remark 7.4 below we shall show that $\mathrm{Li}_n(z)$ on $U_a$ depends on the branch of the logarithm only when $a = 1, \infty$, and make explicit this dependence (cf. [5, Proposition 2.6]).

We will need some further results about $\mathrm{Li}_n(z)$.

**Proposition 2.10.** (1) *For $m \geq 1$ and $z$ in $\mathbb{C}_p$ with $z^m \neq 1$,*

$$\mathrm{Li}_n(z^m) = m^{n-1} \sum_{\zeta^m=1} \mathrm{Li}_n(\zeta z)\,;$$

(2) $\mathrm{Li}_n(z) + (-1)^n \mathrm{Li}_n(z^{-1}) = -\frac{1}{n!}\log^n(z)$.

*Proof.* Those are (the correct version of) Proposition 6.1 and Proposition 6.4(i) of [7]. □

## 3. Method of computation on $U_0$ and $U_\infty$

On $U_0$ we can use the standard expansion in (1.1),

$$\mathrm{Li}_n(t) = \sum_{k=1}^{\infty} \frac{t^k}{k^n}\,, \tag{3.1}$$

which we shall denote by $F_{n,0}(t)$.

*Remark* 3.2. As an immediate consequence of the power series expansion of $\mathrm{Li}_n(z)$ on $U_0$ and the definition of $\mathrm{Li}_n^{(p)}(z)$ in (2.5) we see that on $U_0$

$$\mathrm{Li}_n^{(p)}(z) = \sum_{k\geq 1}{}' \frac{z^k}{k^n}\,, \tag{3.3}$$

where the prime indicates that we only sum over those $k$ for which $p \nmid k$. We can collect terms $z^k/k^n$ in $\mathrm{Li}_n(z) = \sum_{k\geq 1} \frac{z^k}{k^n}$ for which $v_p(k) = m$ and find that

$$\mathrm{Li}_n(z) = \sum_{m\geq 0} \frac{\mathrm{Li}_n^{(p)}(z^{p^m})}{p^{mn}} \tag{3.4}$$

as well.

For the disc $U_\infty$ we use that

$$\mathrm{Li}_n(z) + (-1)^n \mathrm{Li}_n(1/z) = -\frac{1}{n!}\log^n(z)$$

as in part (2) of Proposition 2.10. This reduces the calculation of $\mathrm{Li}_n(z)$ to that of $\mathrm{Li}_n(1/z)$, with $1/z$ in $U_0$, and that of $\log(z)$.

## 4. Method of computation in the generic case

In this section we explain how to compute $\mathrm{Li}_n(z)$ on all residue discs except $U_0$, $U_1$ and $U_\infty$. The residue discs $U_0$ and $U_\infty$ were discussed in the previous section, and $U_1$ will be dealt with in Section 5.

We begin with a well known observation.

**Proposition 4.1.** *Every residue disc other than $U_0$ and $U_\infty$ is $U_\zeta$ for a unique root of unity $\zeta$ of order dividing $p^f-1$ for some $f>0$, known as the* Teichmüller representative *of this residue disc.*

*Proof.* For the residue disc $U_b$ the reduction $\bar{b}$ satisfies $\bar{b}^{p^f-1}=1$ for some $f>0$ because $U_b \neq U_0$ or $U_\infty$. Since $\mathbb{C}_p$ is complete we can apply Hensel's lemma to lift $\bar{b}$ to a unique solution of $x^{p^f-1}=1$ in $U_b$, which is $\zeta$. □

The key observation for the computation of $\mathrm{Li}_n(z)$ is the following.

**Proposition 4.2.** *Suppose that $\zeta \neq 1$ is a $(p^f-1)$-th root of unity. Then*

$$\mathrm{Li}_n(\zeta) = \left(p^{nf}-1\right)^{-1}\left(p^{nf}\mathrm{Li}_n^{(p)}(\zeta) + p^{n(f-1)}\mathrm{Li}_n^{(p)}(\zeta^p) + \cdots + p^n \mathrm{Li}_n^{(p)}(\zeta^{p^{f-1}})\right).$$

*Proof.* This formula is derived in [3] as part of the proof of Corollary 2.2 there. For completeness, we recall the easy proof. For any $z$ in $\mathbb{C}_p$ with $z^{p^k} \neq 1$ we have

$$\sum_{r=0}^{k-1} p^{-rn}\mathrm{Li}_n^{(p)}(z^{p^r}) = \sum_{r=0}^{k-1} p^{-rn}(\mathrm{Li}_n(z^{p^r}) - p^{-n}\mathrm{Li}_n(z^{p^{r+1}})) = \mathrm{Li}_n(z) - p^{-nk}\mathrm{Li}_n(z^{p^k})$$

since the second sum is telescopic. Setting $z=\zeta$ and $k=f$ we have $\zeta^{p^f}=\zeta$; hence

$$\sum_{r=0}^{f-1} p^{-rn}\mathrm{Li}_n^{(p)}(\zeta^{p^r}) = (1-p^{-nf})\mathrm{Li}_n(\zeta) = p^{-nf}(p^{nf}-1)\mathrm{Li}_n(\zeta),$$

so

$$\mathrm{Li}_n(\zeta) = (p^{nf}-1)^{-1}\sum_{r=0}^{f-1} p^{n(f-r)}\mathrm{Li}_n^{(p)}(\zeta^{p^r}),$$

as required. □

Proposition 4.2 implies that if we are able to compute $\mathrm{Li}_n^{(p)}(z)$, then we can find $\mathrm{Li}_n(z)$ at least for $z=\zeta$. For this calculation we use a power series expansion of $\mathrm{Li}_n^{(p)}(z)$ around $\infty$ as in the next result (but see also Remark 8.5). Then Proposition 4.4 below will show how to use the value of $\mathrm{Li}_n(\zeta)$ in order to compute $\mathrm{Li}_n(z)$ for $z$ in $U_\zeta$.

**Proposition 4.3.** *We have* $\mathrm{Li}_n^{(p)}(z) = g_n(1/(1-z))$ *for a power series* $g_n(v)$ *in* $\mathbb{Q}[[v]]$, *convergent for* $v$ *in* $\mathbb{C}_p$ *with* $|v| < p^{1/(p-1)}$. *It is determined inductively by*

$$g_0(v) = v - 1 - \frac{(v-1)^p}{v^p - (v-1)^p},$$
$$g'_{n+1}(v) = -\frac{g_n(v)}{v-v^2} = -\frac{g_n(v)}{v}(1 + v + v^2 + \cdots) \qquad (n \geq 0),$$

*and*

$$g_n(0) = 0 \qquad (n \geq 1).$$

*Proof.* By Theorem 2.7 we can write $\mathrm{Li}_n^{(p)}(z) = g_n(1/(1-z))$ with $g_n(v)$ a power series that converges when $|v| < p^{1/(p-1)}$. To determine the relations satisfied by the $g_n(v)$ we first write $u = 1-z$ and let $f_n(u) = \mathrm{Li}_n^{(p)}(1-u)$ for $n \geq 0$. Using (2.5) the equations in (2.6) become

$$f_0(u) = \frac{1-u}{u} - \frac{(1-u)^p}{1-(1-u)^p} \quad \text{and} \quad f'_{n+1}(u) = -\frac{f_n(u)}{1-u}.$$

Next we set $v = 1/u$ and let $g_n(v) = f_n(1/v)$ to find

$$g_0(v) = v-1-\frac{(v-1)^p}{v^p-(v-1)^p} \quad \text{and} \quad g'_{n+1}(v) = -\frac{g_n(v)}{v-v^2} = -\frac{g_n(v)}{v}(1+v+v^2+\cdots)$$

as required. We then have $g_n(0) = \mathrm{Li}_n^{(p)}(\infty) = 0$ for all $n \geq 0$ by Theorem 2.7(3). Clearly, these relations determine $g_n(v)$ inductively by integration. Because the denominator $v^p-(v-1)^p$ of $g_0(v)$ is a unit in $\mathbb{Z}[[v]]$ we see that $g_0(v)$ is in $\mathbb{Z}[[v]]$ and hence that $g_n(v)$ is in $\mathbb{Q}[[v]]$ for $n \geq 1$. Finally, we observe that $v = 1/(1-z)$. □

**Proposition 4.4.** *Let* $\zeta \neq 1$ *be a* $(p^f-1)$*-th root of unity. For* $z$ *in* $U_\zeta$ *we have that* $\mathrm{Li}_n(z) = F_{n,\zeta}(z-\zeta)$ *for a power series* $F_{n,\zeta}(t)$ *with coefficients in* $\mathbb{Q}_p(\zeta)$. *It converges for* $|t| < 1$ *and can be found inductively by the formulae*

$$F_{0,\zeta}(t) = \frac{\zeta + t}{(1-\zeta) - t} = (1-\zeta)^{-1}\left(\zeta + \frac{t}{1-\zeta} + \frac{t^2}{(1-\zeta)^2} + \cdots\right) \tag{4.5}$$

*and, for* $n \geq 0$,

$$F'_{n+1,\zeta}(t) = \frac{F_{n,\zeta}(t)}{\zeta + t} = \zeta^{-1}F_{n,\zeta}(t)(1 - \zeta^{-1}t + \zeta^{-2}t^2 - \cdots) \tag{4.6}$$

*as well as*

$$F_{n+1,\zeta}(0) = \mathrm{Li}_{n+1}(\zeta). \tag{4.7}$$

*Proof.* The fact that $\mathrm{Li}_n(z)$ is rigid analytic on $U_\zeta$ and therefore has a power series expansion as above was stated in Theorem 2.7(1). The first two formulae are immediate consequences of (2.4). Integration then determines $F_{n+1,\zeta}(t)$ for $n \geq 0$, except for its constant term, which is given by the last equation. Since by Proposition 4.3 $\mathrm{Li}_n^{(p)}(\zeta)$ is in $\mathbb{Q}_p(\zeta)$ the same holds for $\mathrm{Li}_n(\zeta)$ by Proposition 4.2. The claim about the coefficients is then clear from the inductive formulae. □

For use in some of the estimates in the following sections we also prove a few results about the absolute values of $\mathrm{Li}_n^{(p)}(z)$ and $\mathrm{Li}_n(z)$ (cf. [3]). Note that if $|z| < 1$, then $|\mathrm{Li}_n^{(p)}(z)| = |z|$ by (3.3).

**Proposition 4.8.** *If $z$ in $\mathbb{C}_p$ satisfies $|z-1|=1$, then $|\mathrm{Li}_n^{(p)}(z)| \leq 1$.*

*Proof.* This is a slight generalization of [3, Proposition 2.1], with the same proof. We use a formula found by Coleman [7, Lemma 7.2],

$$\mathrm{Li}_n^{(p)}(z) = \int_{\mathbb{Z}_p^*} x^{-n} d\mu_z(x)\,,$$

where $\mu_z$ is the measure on $\mathbb{Z}_p$ such that $\mu_z(a+p^k\mathbb{Z}_p) = \frac{z^a}{1-z^{p^k}}$ for $a = 1, \ldots, p^k$. Since for the specified values of $z$ this measure takes values with absolute value at most 1, the same holds for $\mathrm{Li}_n^{(p)}(z)$. □

**Corollary 4.9** ([3, Corollary 2.2])**.** *If $\zeta \neq 1$ is a root of unity of order prime to $p$, then $\mathrm{Li}_n(\zeta)$ is in $p^n\mathbb{Z}_p[\zeta]$.*

*Proof.* We have that $\mathrm{Li}_n^{(p)}(\zeta)$ is in $\mathbb{Q}_p(\zeta)$ by Proposition 4.3, and by Proposition 4.8 we have $|\mathrm{Li}_n^{(p)}(\zeta)| \leq 1$ so that $\mathrm{Li}_n^{(p)}(\zeta)$ is in $\mathbb{Z}_p[\zeta]$. The result is now immediate from Proposition 4.2. □

**Corollary 4.10.** *If $\zeta$ is a root of unity of order $p^k m$ with $m > 1$ not divisible by $p$, then $|\mathrm{Li}_n(\zeta)| \leq p^{(k-1)n}$.*

*Proof.* For $k = 0$ this is part of Corollary 4.9. For $k > 0$ it then follows by induction since $\mathrm{Li}_n(\zeta) = p^{-n}\mathrm{Li}_n(\zeta^p) + \mathrm{Li}_n^{(p)}(\zeta)$ and $|\mathrm{Li}_n^{(p)}(\zeta)| \leq 1$ by Proposition 4.8. □

## 5. Method of computation on $U_1$

To compute $\mathrm{Li}_n(z)$ for $z \neq 1$ in $U_1$ we use the following result.

**Proposition 5.1** ([7, Proposition 7.1])**.** *For $n \geq 2$ the function*

$$E_n(z) = \mathrm{Li}_n(z) - \frac{1}{n-1}\log(z)\mathrm{Li}_{n-1}(z) \tag{5.2}$$

*extends to a rigid analytic function on $U_1$.*

It is then clear that $E_n(z)$ is defined for $z \neq 0$. Moreover, Proposition 2.10(1) together with the identities $\log(z^m) = m\log(z)$ and $\log(\zeta z) = \log(z)$ for a root of unity $\zeta$ implies that we have a distribution relation

$$E_n(z^m) = m^{n-1}\sum_{\zeta^m=1} E_n(\zeta z) \tag{5.3}$$

for $m \geq 1$ and $z$ in $\mathbb{C}_p^*$. In particular

$$E_n(z^2) = 2^{n-1}(E_n(z) + E_n(-z))\,. \tag{5.4}$$

**Proposition 5.5.** *On $U_1$ the functions $E_n(z)$ are independent of the branch of the logarithm.*

*Proof.* It is easy to check that for $n \geq 3$ we have $(n-1)E_n'(z) = (n-2)E_{n-1}(z)/z$. Since $E_n(z)$ is rigid analytic on $U_1$ as stated above, the statement follows by induction provided that $E_n(1)$ is independent of the branch. Taking $m = p-1$ in (5.3) we see that $E_n(1)$ is determined by the $E_n(\zeta)$ where $\zeta^{p-1} = 1$ and $\zeta \neq 1$. But $E_n(\zeta) = \mathrm{Li}_n(\zeta)$ for such $\zeta$ by (5.2), and from Proposition 4.2 and Theorem 2.7 we find that those values are independent of the branch of the logarithm. □

The $E_m(z)$ for $z$ in $U_1$ are much easier to deal with than the $\mathrm{Li}_m(z)$, and we express $\mathrm{Li}_n(z)$ in terms of the $E_m(z)$ and logarithms.

**Proposition 5.6.** *We have, for $z \neq 1$ in $U_1$ and $n \geq 2$,*

$$\mathrm{Li}_n(z) = \frac{1}{(n-1)!}\log^{n-1}(z)\mathrm{Li}_1(z) + \sum_{j=2}^{n}\frac{(j-1)!}{(n-1)!}\log^{n-j}(z)E_j(z)\,.$$

*Proof.* For $n \geq 2$ we get from (5.2) that

$$(n-1)!\,E_n(z) = (n-1)!\,\mathrm{Li}_n(z) - (n-2)!\log(z)\mathrm{Li}_{n-1}(z)\,.$$

Setting $E_1(z) = \mathrm{Li}_1(z)$ we have an equality of generating power series in $T$,

$$\sum_{n\geq 1}(n-1)!\,E_n(z)T^n = (1-\log(z)T)\Big(\sum_{n\geq 1}(n-1)!\,\mathrm{Li}_n(z)T^n\Big)\,,$$

so that

$$\sum_{n\geq 1}(n-1)!\,\mathrm{Li}_n(z)T^n = \Big(\sum_{n\geq 1}(n-1)!\,E_n(z)T^n\Big)(1+\log(z)T+\log^2(z)T^2+\cdots),$$

and the result follows easily. □

*Remark* 5.7. Because $\log(z)$ and $E_n(z)$ are rigid analytic on $U_1$ the second summand of $\mathrm{Li}_n(z)$ in Proposition 5.6 is rigid analytic there. But $\mathrm{Li}_1(z) = -\log(1-z)$ is not rigid analytic around 1, hence neither are the first summand and $\mathrm{Li}_n(z)$ itself.

However, for $n \geq 2$ we can extend $\mathrm{Li}_n(z)$ to the whole of $\mathbb{C}_p$ by putting $\mathrm{Li}_n(1) = E_n(1)$ (which is independent of the branch of the logarithm by Proposition 5.5). If $F \subset \mathbb{C}_p$ is any field that is finitely ramified over $\mathbb{Q}_p$, then $\log(z)$ is bounded on $F^*$ by the formulae in Remark 2.2 (see Remark 8.1), so by Proposition 5.6 this extended $\mathrm{Li}_n(z)$ is continuous on $F$. It follows from this continuity that part (1) of Proposition 2.10 holds for all $z$ in $\mathbb{C}_p$ (cf. [7, Corollary 7.1a]) and part (2) for all $z \neq 0$ in $\mathbb{C}_p$.

We deal with the two summands in the expression for $\mathrm{Li}_n(z)$ in Proposition 5.6 separately. Computing the logarithms is standard, and we develop the other function as a power series around 1 using iterated integration as described in the next proposition. The constant of integration is expressed in terms of $\mathrm{Li}_n(-1)$, which we can compute using Propositions 4.2 and 4.3 if $p \neq 2$. But if $p = 2$, then $-1$ is outside of the set in Proposition 2.7(3) and we give a different formula that we can calculate as we go along.

**Proposition 5.8.** *For $n \geq 1$ set $G_n(t) = \log^n(1+t)/n!$, and for $n \geq 2$ let*

$$H_n(t) = \sum_{j=2}^{n}\frac{(j-1)!}{(n-1)!}\log^{n-j}(1+t)E_j(1+t)\,.$$

*Then $G_n(t)$ and $H_n(t)$ for $|t| < 1$ are given by power series in $\mathbb{Q}_p[[t]]$, with $H_n(t)$ satisfying*

$$H_2'(t) = 1 - t/2 + t^2/3 - \cdots\,, \tag{5.9}$$

$$H_n'(t) = \frac{H_{n-1}(t)}{1+t} + \frac{G_{n-1}(t)}{t} \quad (n \geq 3) \tag{5.10}$$

*as well as*

$$H_n(0) = 2^{n-1}\mathrm{Li}_n(-1)/(1-2^{n-1})\,.$$

*If $p = 2$, then also*

$$H_n(0) = \frac{2^{n-1}}{1-2^n}(H_n(-2) - H_n(0))\,. \tag{5.11}$$

*Proof.* That the $G_n(t)$ for $|t| < 1$ are given by power series in $\mathbb{Q}[[t]] \subset \mathbb{Q}_p[[t]]$ is well-known. By Proposition 5.1 we know that the $E_m(t+1)$ for $m = 2, \dots, n$ are given by power series in $\mathbb{C}_p[[t]]$ that converge for $|t| < 1$ so that the same holds for $H_n(t)$. We shall now first prove the inductive formulae and then conclude that the power series are actually in $\mathbb{Q}_p[[t]]$.

From (2.3) we have that $E_2'(z) = -\log(z)/(1-z)$ so that $H_2'(t) = E_2'(t+1) = \log(1+t)/t$ which gives the first formula. For $m \geq 3$ we have $(m-1)E_m'(z) = (m-2)E_{m-1}(z)/z$ so that $H_n'(t)$ for $n \geq 3$ is given by

$$\sum_{j=3}^{n-1} \frac{(j-1)!}{(n-1)!}\left[(n-j)\frac{\log^{n-j-1}(1+t)}{1+t}E_j(1+t) + \frac{j-2}{j-1}\log^{n-j}(1+t)\frac{E_{j-1}(1+t)}{1+t}\right]$$
$$+ \frac{\log^{n-1}(1+t)}{(n-1)!\,t} + (n-2)\frac{\log^{n-3}(1+t)}{(n-1)!\,(1+t)}E_2(1+t) + \frac{n-2}{n-1}E_{n-1}(1+t)$$

and collecting powers of $\log(1+t)$ this becomes

$$\sum_{j=2}^{n-1} \frac{(j-1)!}{(n-1)!}\,[(n-j)+(j-1)]\frac{\log^{n-j-1}(1+t)}{1+t}E_j(1+t) + \frac{\log^{n-1}(1+t)}{(n-1)!\,t}\,,$$

proving the second formula.

As for the constant terms, we see from (5.4) that $E_n(1) = 2^{n-1}(E_n(1)+E_n(-1))$. Therefore $H_n(0) = E_n(1) = 2^{n-1}E_n(-1)/(1-2^{n-1})$, and $E_n(-1) = \mathrm{Li}_n(-1)$ since $\log(-1) = 0$. If $p = 2$, then $-1$ is in $U_1$ so that the definition of $H_n(t)$ gives $H_n(-2) = E_n(-1) = \mathrm{Li}_n(-1)$ and this leads immediately to the alternative formula for $H_n(0)$.

Finally, we prove that the coefficients of the $H_n(t)$ are in $\mathbb{Q}_p$. For $p \neq 2$ it follows from Proposition 4.3 that $\mathrm{Li}_n^{(p)}(-1)$ is in $\mathbb{Q}_p$ for $n \geq 0$. Then Proposition 4.2 (with $f = 1$) shows that $\mathrm{Li}_n(-1)$ is in $\mathbb{Q}_p$, so the same holds for $H_n(0)$ by what we proved in the previous paragraph. Therefore, since $H_2'(t)$ is in $\mathbb{Q}_p[[t]]$ by (5.9), $H_2(t)$ is in $\mathbb{Q}_p[[t]]$. For $n > 2$ we conclude by induction on $n$ using (5.10) since $G_{n-1}(t)/t$ is in $\mathbb{Q}_p[[t]]$ for such $n$. If $p = 2$, then we prove by induction on $n$ that $H_n'(t)$ is in $\mathbb{Q}_2[[t]]$ and $H_n(0)$ is in $\mathbb{Q}_2$. For $n = 2$ it is clear from (5.9) that we can find $\widetilde{H}_2(t)$ in $\mathbb{Q}_2[[t]]$ with $\widetilde{H}_2'(t) = H_2'(t)$ and $\widetilde{H}_2(0) = 0$, so $H_2(t) = H_2(0) + \widetilde{H}_2(t)$. Then $H_2(0)$ is in $\mathbb{Q}_2$ by (5.11) since $H_2(-2) - H_2(0) = \widetilde{H}_2(-2)$ is in $\mathbb{Q}_2$. Hence $H_2(t)$ is in $\mathbb{Q}_2[[t]]$. For $n > 2$ the proof proceeds similarly, writing $H_n(t) = H_n(0) + \widetilde{H}_n(t)$ with, inductively, $\widetilde{H}_n(t)$ in $\mathbb{Q}_2[[t]]$ by (5.10). □

*Remark* 5.12. (1) It follows from the definition of $E_m(z)$ and Proposition 2.10(2) that $E_n(z) + (-1)^n E_n(1/z) = \log^n(z)/(n!\,(n-1))$. Therefore $E_n(1)$, $E_n(-1)$, $\mathrm{Li}_n(1)$, $\mathrm{Li}_n(-1)$ and $H_n(0)$ are all 0 when $n \geq 2$ is even.

(2) For $p \neq 2$ Proposition 4.2 with $\zeta = -1$ simplifies to $\mathrm{Li}_n(-1) = \frac{p^n}{p^n-1}\mathrm{Li}_n^{(p)}(-1)$ so that $H_n(0) = \frac{2^{n-1}p^n}{(1-2^{n-1})(p^n-1)}\mathrm{Li}_n^{(p)}(-1)$.

## 6. Estimates

In this section we provide estimates for the valuations of the coefficients in the power series $g_n(v)$ of Proposition 4.3, $F_{n,\zeta}(t)$ of Proposition 4.4 and $H_n(t)$ of Proposition 5.8. We shall use these in Section 7 to know how many terms of those power series we have to calculate in order to compute $\mathrm{Li}_n(z)$ up to a specified precision for a given $z \neq 1$ in $\mathbb{C}_p$.

Many expressions in Sections 6 through 8 contain the real logarithm with base $p$, denoted $\log_p$, which should not be confused with the chosen branch of the $p$-adic logarithm, denoted log. In order to avoid another possible confusion we denote the real logarithm by ln.

For the coefficients of $g_n(v)$ we have the following result.

**Proposition 6.1.** *For $n \geq 1$ let*

$$c(n,p) = \frac{p}{p-1} - \frac{n-1}{\ln(p)} + (n-1)\log_p\left(\frac{n(p-1)}{\ln(p)}\right) + \log_p\left(\frac{2p(p-1)n}{\ln(p)}\right).$$

*If*

$$g_n(v) = a_{n,1}v + a_{n,2}v^2 + \cdots,$$

*then*

$$v_p(a_{n,k}) \geq \max\left(0, \frac{k}{p-1} - \log_p(k) - c(n,p)\right).$$

*Proof.* We first show that $v_p(a_{n,k}) \geq 0$. For this we recall that for a power series $f(z) = \sum_i b_i z^i$ converging on the closed unit disc, we have that $\max|b_i| = \max_{|z|=1}|f(z)|$, where $z$ must be considered in the algebraic closure of the field of coefficients (see [10, Example 3.3.2]), which will be $\mathbb{Q}_p$ in our case. It thus suffices to show that $g_n(z) = \mathrm{Li}_n^{(p)}(1-z^{-1})$ takes on integral values when $|z| = 1$. But then $|(1-z^{-1})-1| = 1$ so that we can apply Proposition 4.8.

Next we estimate $v_p(a_{0,k})$. Recall from Proposition 4.3 that

$$g_0(v) = v - 1 - \frac{(v-1)^p}{v^p - (v-1)^p} = v - 1 + (v-1)^p \sum_{i=0}^{\infty} (pf(v))^i,$$

where $v^p - (v-1)^p = 1 - pf(v)$ for some polynomial $f(v)$ in $\mathbb{Z}[v]$ of degree $p-1$. Then any term contributing to $v^k$ in $g_0(v)$ for $k > 1$ will come from a product containing $(pf(v))^i$ with $i \geq \lceil (k-p)/(p-1) \rceil$, where $\lceil x \rceil$ is the smallest integer greater than or equal to $x$. Therefore, also for $k = 1$,

$$v_p(a_{0,k}) \geq \left\lceil \frac{k-p}{p-1} \right\rceil. \tag{6.2}$$

We now prove the estimate for $n \geq 1$. By Proposition 4.3 we have

$$\begin{aligned} g'_{n+1}(v) &= -\frac{g_n(v)}{v}(1 + v + v^2 + \cdots) \\ &= -a_{n,1} - (a_{n,1} + a_{n,2})v - (a_{n,1} + a_{n,2} + a_{n,3})v^2 - \cdots \end{aligned}$$

and consequently $k a_{n+1,k} = -(a_{n,1} + \cdots + a_{n,k})$ for $k \geq 1$. Substituting $v = 1$, which is in the range of convergence for $g_n$, we find

$$\sum_{i=1}^{\infty} a_{n,i} = g_n(1) = \mathrm{Li}_n^{(p)}(0) = 0.$$

It follows that $ka_{n+1,k} = a_{n,k+1} + a_{n,k+2} + \cdots$. Therefore

$$v_p(a_{n+1,k}) \geq \min_{j \geq k+1} \{v_p(a_{n,j}) - v_p(k)\}\,.$$

Iterating this and using (6.2) we obtain

$$\begin{aligned} v_p(a_{n,k}) &\geq \min_{k=j_0<j_1<j_2<\cdots<j_n} \left\{ \left\lceil \frac{j_n - p}{p-1} \right\rceil - \sum_{i=0}^{n-1} v_p(j_i) \right\} \\ &\geq \min_{k=j_0<j_1<j_2<\cdots<j_n} \left\{ \frac{j_n - p}{p-1} - \sum_{i=0}^{n-1} v_p(j_i) \right\}. \end{aligned}$$

We shall bound the last expression from below. We do this by first considering possible values of $j_n$. Suppose that $k + p^l \leq j_n < k + p^{l+1}$ for some integer $l \geq 0$. We then have the lower bound

$$\frac{j_n - p}{p-1} \geq \frac{k + p^l - p}{p-1}\,. \tag{6.3}$$

We now bound $\sum_{i=0}^{n-1} v_p(j_i)$ from above when $k \leq j_0 < \cdots < j_{n-1} < k + p^{l+1} - 1$. Clearly, among the $p^{l+1}$ consecutive integers $k, \ldots, k + p^{l+1} - 1$ there is only one integer divisible by $p^{l+1}$, and its valuation is bounded by $\log_p(k + p^{l+1})$. The remaining integers in this range are not divisible by $p^{l+1}$, and their valuations are bounded by $l$. Thus, we have

$$\sum_{i=0}^{n-1} v_p(j_i) \leq (n-1)l + \log_p(k + p^{l+1})\,. \tag{6.4}$$

Combining the estimates (6.3) and (6.4) and taking the minimum over all possible $l$'s we finally arrive at the estimate

$$\begin{aligned} v_p(a_{n,k}) &\geq \min_{0 \leq l \in \mathbb{Z}} \left\{ \frac{k + p^l - p}{p-1} - (n-1)l - \log_p(k + p^{l+1}) \right\} \\ &\geq \min_{0 \leq l \in \mathbb{R}} \left\{ \frac{k + p^l - p}{p-1} - (n-1)l - \log_p(k + p^{l+1}) \right\}. \end{aligned} \tag{6.5}$$

Computing this last minimum is a standard problem. We have

$$\frac{\mathrm{d}}{\mathrm{d}l} \left( \frac{k + p^l - p}{p-1} - (n-1)l - \log_p(k + p^{l+1}) \right) = \frac{\ln(p) \cdot p^l}{p-1} - (n-1) - \frac{p^{l+1}}{k + p^{l+1}}\,.$$

This derivative is clearly positive for large $l$ and is negative for $l = 0$ when $n \geq 2$. Consequently, for $n \geq 2$ it must vanish at the value of $l$ where the right-hand side of (6.5) attains its minimal value, so that we get

$$\frac{\ln(p) \cdot p^l}{p-1} = n - 1 + \frac{p^{l+1}}{k + p^{l+1}}\,.$$

Since the last summand is always between 0 and 1 we obtain the inequalities

$$n > \frac{\ln(p) \cdot p^l}{p-1} > n - 1\,,$$

which implies that $l < \log_p(n(p-1)/\ln(p))$, $p^l/(p-1) > (n-1)/\ln(p)$ and $p^{l+1} < p(p-1)n/\ln(p)$.

We observe that those inequalities also hold if $n = 1$ and $l = 0$ so that they hold where the right-hand side of (6.5) attains its minimum. Using them, as well as $\ln(x+y) \le \ln(x) + \ln(2y)$ for $x$, $y \ge 1$, we find that $v_p(a_{n,k})$ is at least equal to

$$\begin{aligned}&\frac{k-p}{p-1} + \frac{n-1}{\ln(p)} - (n-1)\log_p\left(\frac{n(p-1)}{\ln(p)}\right) - \log_p(k) - \log_p\left(\frac{2p(p-1)n}{\ln(p)}\right)\\ &= \frac{k}{p-1} - \log_p(k) - c(n,p)\end{aligned}$$

as required. □

*Remark* 6.6. Proposition 6.1 implies that $g_n(v)$ converges for $|v| < p^{1/(p-1)}$, as stated in Theorem 2.7(3) and Proposition 4.3. The bound seems to have the right behaviour, and only the constant $c(n,p)$ may possibly be improved.

We now move on to estimates concerning the $F_{n,\zeta}(t)$'s that were introduced in Proposition 4.4. It is clear from (3.1) that the coefficient of $t^k$ in $F_{n,0}(t)$ has valuation at least $-n\log_p(k)$ for all $k \ge 1$. For the corresponding statement for the $F_{n,\zeta}(t)$'s (with $\zeta \ne 1$ a root of unity of order relatively prime to $p$) we have to work a little more.

**Proposition 6.7.** *Let $\zeta \ne 1$ be a $(p^f-1)$-th root of unity and write*

$$F_{n,\zeta}(t) = a_{n,0} + a_{n,1}t + a_{n,2}t^2 + \cdots$$

*in $\mathbb{Q}_p(\zeta)[[t]]$. Then $a_{n,0}$ is in $p^n\mathbb{Z}_p[\zeta]$, and for $k \ge 1$ we have $v_p(a_{n,k}) \ge -n\log_p(k)$.*

*Proof.* By Corollary 4.9 $a_{n,0} = \mathrm{Li}_n(\zeta)$ lies in $p^n\mathbb{Z}_p[\zeta]$. We proceed to prove the other statement by induction on $n$. For $n = 0$ we have that $\mathrm{Li}_0(z) = \frac{z}{1-z}$ and so $F_{0,\zeta}(t) = \frac{\zeta+t}{(1-\zeta)-t}$. Because $\zeta$ does not reduce to 1 by assumption $(1-\zeta)-t$ is a unit in $\mathbb{Z}_p[\zeta][[t]]$, so $F_{0,\zeta}(t)$ is in $\mathbb{Z}_p[\zeta][[t]]$. For $n \ge 1$ we see from (4.6) that

$$ka_{n+1,k} = -\sum_{j=0}^{k-1}(-\zeta)^{j-k}a_{n,j}\,. \tag{6.8}$$

Hence $k\,a_{n+1,k}$ is a sum of elements with valuations $v_p(a_{n,j})$, $0 \le j \le k-1$, and so for $k \ge 1$, $v_p(a_{n+1,k}) \ge \min_{j=0,\ldots,k-1}\{v_p(a_{n,j})\} - v_p(k) \ge -n\log_p(k) - \log_p(k)$. □

*Remark* 6.9. The proof of Proposition 6.7 actually shows that we have the slightly better estimate $v_p(a_k) \ge -\log_p\left(\frac{k!}{\max(0,k-n)!}\right)$ for all $k \ge 0$.

Finally, we consider the series $H_n(t)$ for $n \ge 2$ that were introduced in Proposition 5.8. For this we need a lemma concerning the $G_n(t) = \log^n(1+t)/n!$ introduced in the same proposition.

**Lemma 6.10.** *For $n \ge 1$ write*

$$G_n(t) = a_{n,1}t + a_{n,2}t^2 + a_{n,3}t^3 + \cdots\,.$$

*Then $v_p(a_{n,k}) \ge -n\log_p(k)$ for all $k \ge 1$.*

*Proof.* We proceed by induction on $n$, the case $n = 1$ being clear. For $n \ge 2$ we have $G_n'(t) = G_{n-1}(t)/(1+t)$ so that, for $k \ge 1$,

$$ka_{n,k} = \left((-1)^{k-2}a_{n-1,1} + (-1)^{k-3}a_{n-1,2} + \cdots + a_{n-1,k-1}\right),$$

and the statement follows easily (cf. the proof of Proposition 6.7). □

**Proposition 6.11.** *For $n \geq 2$ write*

$$H_n(t) = b_{n,0} + b_{n,1}t + b_{n,2}t^2 + \cdots$$

*in $\mathbb{Q}_p[[t]]$. Then $v_p(b_{n,0}) \geq n - v_p(n-1) - \epsilon_p$, where $\epsilon_p = 2$ for $p = 2$ and $\epsilon_p = 1$ otherwise. Moreover, $v_p(b_{n,k}) \geq -n\log_p(k)$ for all $k \geq 1$.*

*Proof.* We begin with the statement for $k = 0$. It follows easily from (5.3) and Corollary 4.9 that

$$v_p(H_n(0)) = v_p(E_n(1)) \geq n - \min_{p\nmid m>1}\{v_p(m^{n-1}-1)\}.$$

Now $m^{n-1}-1$ will be divisible by $p^s$ for all $m$ relatively prime to $p$ precisely when the exponent of $(\mathbb{Z}/p^s)^*$ divides $n-1$. Therefore any such $s$ satisfies $s \leq v_p(n-1)+\epsilon_p$ so that $v_p(H_n(0)) \geq n - v_p(n-1) - \epsilon_p$.

We now observe that $H_2(t) = -\sum_{k\geq 1}(-t)^k/k^2$ by Proposition 5.8 and Remark 5.12(1) so that the other statement holds if $n = 2$. If $n \geq 3$, then (5.10) gives

$$kb_{n,k} = ((-1)^{k-1}b_{n-1,0} + (-1)^{k-2}b_{n-1,1} + \cdots + b_{n-1,k-1}) + a_{n-1,k}$$

with $a_{n-1,k}$ as in Lemma 6.10, hence $v_p(a_{n-1,k}) \geq -(n-1)\log_p(k)$. Again the statement follows by induction on $n$ because $(n-1) - v_p(n-2) - \epsilon_p \geq 0 \geq -\log_p(k)$. □

## 7. The algorithm

In this section we use the material from the previous sections in order to give an algorithm for computing $\mathrm{Li}_n(z)$ for $n \geq 2$ and $z \neq 1$ up to a given precision and analyze its efficiency.

First of all we formalize the notion of "up to a given precision".

**Definition 7.1.** (1) For any number $\alpha$ in $\mathbb{C}_p$ we say that we know $\alpha$ up to precision $N$ if we have $\beta$ in $\mathbb{C}_p$ such that $v_p(\alpha - \beta) > N$.

(2) We say that we know $\alpha \neq 0$ in $\mathbb{C}_p$ up to relative precision $N$ if we have $\beta$ in $\mathbb{C}_p$ such that $v_p(\beta/\alpha - 1) > N$.

*Remark* 7.2. (1) Note that those notions are absolute; even if $\alpha$ is in a finite extension of $\mathbb{Q}_p$ they do not take the ramification of this extension into account.

(2) For $\alpha$ and $\beta$ as in the first part of the definition we shall refer to $\beta$ as an approximation of $\alpha$ up to precision $N$.

(3) If we know $\alpha \neq 0$ up to precision $N$, then we know $\alpha$ up to relative precision $N - v_p(\alpha)$, and conversely.

(4) If $z \neq 0$ is known up to relative precision $N \geq 0$, then so is $1/z$. In particular, if we know $z \neq 0$ up to precision $N > v_p(z)$, then we know $z$ and $1/z$ up to relative precision $N - v_p(z)$, and $1/z$ up to precision $N - 2v_p(z)$.

We assume that we want to compute $\mathrm{Li}_n(z)$ up to precision $N > 0$ for $z \neq 1$ in a complete subfield $F$ of $\mathbb{C}_p$. If $z$ in $F$ does not lie in $U_0$, $U_1$ or $U_\infty$, then it lies in $U_\zeta$ for some Teichmüller representative $\zeta \neq 1$. Since $F$ is complete one sees as in the proof of Proposition 4.1 that $\zeta$ lies in $F$.

We shall also assume that we know $z$ up to precision $N' > v_p(z)$ so that we can at least decide in which residue disc $z$ lies and, in fact, we know $v_p(z)$. In Algorithm 7.10 we will also give a value of $N'$ that suffices for the computation of $\mathrm{Li}_n(z)$ up to precison $N$.

*Remark* 7.3. For the algorithm it is not necessary to assume that $F$ is a finite extension of $\mathbb{Q}_p$, but with that assumption it is possible to give universal estimates (see Remark 8.1) and to quantify its efficiency (see Theorem 8.2). If we want to know $\mathrm{Li}_n(z)$ up to precision $N$ for arbitrary $z$ in $\mathbb{C}_p$, then from the algorithm we can determine $N'$ such that for an approximation $\tilde{z}$ of $z$ up to precision $N'$, $\mathrm{Li}_n(\tilde{z})$ is an approximation of $\mathrm{Li}_n(z)$ up to precision $N$. By taking this $\tilde{z}$ in $\overline{\mathbb{Q}}_p$ we reduce to calculations in $\mathbb{Q}_p(\tilde{z})$, a finite extension of $\mathbb{Q}_p$ and a complete field.

*Remark* 7.4. We shall now show that $\mathrm{Li}_n(z)$ is in $F$ because $F$ is complete, and clarify how $\mathrm{Li}_n(z)$ depends on the branch of the logarithm (see Definition 2.1 and Remark 2.2). (The latter was also made explicit in [5, Proposition 2.6] by a different method.)

It is clear from (3.1) that $F_{n,0}(t)$ lies in $\mathbb{Q}[[t]]$, so that $\mathrm{Li}_n(z)$ for $z$ in $U_0$ lies in $F$ and is independent of the branch of the logarithm.

For $z \neq \infty$ in $U_\infty$ it follows from Proposition 2.10(2) that $\mathrm{Li}_n(z)$ is in $F$ provided we use a branch of the logarithm for which $\log(p)$ is in $F$. The dependence on this branch is also clear from this.

If $z$ in $U_\zeta$, where $\zeta \neq 1$ is a $(p^f-1)$-th root of unity for some $f > 0$, then by Proposition 4.4 the coefficients of $F_{n,\zeta}(t)$ are in $\mathbb{Q}_p(\zeta) \subseteq F$ so that $\mathrm{Li}_n(z)$ lies in $F$. Since the statements of Propositions 4.2, 4.3 and 4.4 do not depend on the branch of the logarithm, neither does $\mathrm{Li}_n(z)$ for such $z$.

For $z \neq 1$ in $U_1$ it is clear that $\mathrm{Li}_1(z) = -\log(1-z)$ is in $F$ if $\log(p)$ is, and the dependence on the branch of the logarithm is clear as well. For $n \geq 2$, we use Propositions 5.6 and 5.8 to write $\mathrm{Li}_n(z) = H_n(z-1) - \log^{n-1}(z)\log(1-z)/(n-1)!$. From its definition and Proposition 5.5 we have that $H_n(z-1)$ is independent of the branch of the logarithm. Moreover, from Proposition 5.8 we see that it is in $F$. So $\mathrm{Li}_n(z)$ is in $F$ if $\log(p)$ is, and the dependence of $\mathrm{Li}_n(z)$ on the branch of the logarithm is also explicit since only $\log(1-z)$ depends on it. Finally, for $z = 1$ and $n \geq 2$ we defined $\mathrm{Li}_n(1)$ in Remark 5.7 as $E_n(1) = H_n(0)$, which is in $\mathbb{Q}_p$ by Proposition 5.8 and is independent of the branch of the logarithm by Remark 5.7.

Before giving the algorithm, we describe two special cases that have to be dealt with separately, namely $z = 0$ and $z = 1$.

*Remark* 7.5. Note that we can know $z$ in $\mathbb{C}_p$ up to precision $N' > v_p(z)$ only when $z \neq 0$, which we shall assume in Algorithm 7.10 below. However, clearly $\mathrm{Li}_n(0) = 0$, and if we know that $|z| < p^{-N'} \leq 1$, then $|\mathrm{Li}_n(z)| < \max_{m\geq 0}\{p^{mn-N'p^m}\}$ by (3.4) because $|\mathrm{Li}_n^{(p)}(z)| = |z|$ when $|z| < 1$. If $n \leq N'\ln(p)$, then this maximum is attained for $m = 0$ and equals $p^{-N'}$, but if $n > N'\ln(p)$, then it may be much bigger.

For $z = 1$ the problem is of a different nature. Although we defined $\mathrm{Li}_n(1)$ for $n \geq 2$ in Remark 5.7, in order to be able to bound $\mathrm{Li}_n(z) - \mathrm{Li}_n(1)$ if $z = 1$ up to its precision, we assume that $F$ has finite ramification index over $\mathbb{Q}_p$.

*Remark* 7.6. (1) For $n \geq 2$ we have $\mathrm{Li}_n(1) = 2^{n-1}\mathrm{Li}_n(-1)/(1-2^{n-1})$ (see Remark 5.7 and Proposition 2.10(1)), which we can compute up to any desired precision using Algorithm 7.10 below. Of course, if $n$ is even, then this value is zero by Remark 5.12(1).

(2) If $|z-1| < p^{-N'} \leq 1$, $z$ is in a subfield of $\mathbb{C}_p$ of finite ramification index $e$, and $n \geq 2$, then $\mathrm{Li}_n(z) = \mathrm{Li}_n(1)$ up to precision

$$\min\{n\log_p(N'/n), (n-1)\log_p(N') - v_p((n-1)!) - v_p(e) + \min\{v_p(\log(p)), -\log_p(e)\}\}.$$

If $N'\ln(p) \geq n$, then this holds up to precision

$$\min\{N', (n-1)N' - v_p((n-1)!) - v_p(e) + \min\{v_p(\log(p)), -\log_p(e)\}\}.$$

Namely, combining Propositions 5.6 and 5.8 we have, for $z \neq 1$ in $U_1$,

$$\mathrm{Li}_n(z) = H_n(z-1) - \frac{\log^{n-1}(z)\log(1-z)}{(n-1)!}, \tag{7.7}$$

and in Remark 5.7 we put $\mathrm{Li}_n(1) = E_n(1) = H_n(0)$ . Thus we are really interested in a lower bound for the $p$-adic valuation of

$$H_n(t) - H_n(0) - \frac{\log^{n-1}(1+t)\log(-t)}{(n-1)!} \tag{7.8}$$

when for $t = z-1$ we have $v_p(t) > N' \geq 0$. By Proposition 6.11 we have

$$v_p(H_n(t) - H_n(0)) > \min_{k\geq 1}\{kN' - n\log_p(k)\},$$

and, similarly, $v_p(\log(1+t)) > \min_{k\geq 1}\{kN' - \log_p(k)\}$. By our assumption on the ramification, $ev_p(t)$ is a positive integer $a$ and

$$\log(-t) = \log(t) = e^{-1}(a\log(p) + \log(t'))$$

with $t' = t^e/p^a$ having absolute value 1. Since $\log(\eta) = 0$ for any root of unity $\eta$ we may assume $t'$ is in $U_1$, hence satisfies $v_p(t'-1) \geq 1/e$. Then an estimate for $\log(t')$ similar to that for $\log(1+t)$ gives

$$v_p(\log(t)) \geq \min\{v_p(\log(p)), \min_{k\geq 1}\{ke^{-1} - \log_p(k)\}\} - v_p(e).$$

(For a slightly different estimate for this see Remark 8.1.) Our statements then follow from (7.8) by using the following lemma for the minima in our estimates.

**Lemma 7.9.** *For $p$ prime and $C, c > 0$, $\min_{k\geq 1}\{Ck - c\log_p(k)\} > c\log_p(C/c)$. If $C\ln(p) \geq c$, then this minimum equals $C$.*

*Proof.* Differentiating $Ck - c\log_p(k)$ with respect to $k$ we see that this function has a unique minimum on the positive reals at $k_0 = c/(C\ln(p))$, and that if $k_0 \leq 1$, then our original minimum is at $k = 1$, hence equals $C$. If $k_0 > 1$, then the minimum on the positive reals equals $\frac{c}{\ln(p)}(1 - \ln(c) + \ln(C) + \ln(\ln(p))) > c\log_p(C/c)$ since $\ln(\ln(p)) > -1$ for all primes $p$. □

We now give the algorithm for computing $\mathrm{Li}_n(z)$ up to precision $N$ for $z \neq 0, 1$, while also giving a sufficient precision for $z$ for this. The various steps, in which we consider (approximations of) truncations of $F_{n,\zeta}(t)$, $g_n(v)$ and $H_n(t)$ by ignoring terms of degree at least $\mathsf{tsl}$, $\mathsf{gsl}$ and $\mathsf{hsl}$ respectively, will be justified afterwards. We assume that the fixed branch of the logarithm, $\log(z)$, is readily computable.

**Algorithm 7.10.** In order to compute $\mathrm{Li}_n(z)$ for $z \neq 0, 1$ in $F$ and $n \geq 2$ up to precision $N > 0$ we first determine in which residue disc $z$ lies and then do the following.

(1) If $z$ is in $U_0$, then we find $M \geq 0$ such that $p^m v_p(z) - mn > N$ for all $m > M$. For each $m = 0, \ldots, M$ we find $\mathsf{tsl}_m \geq 1$ such that $kp^m v_p(z) - mn > N$ for $k \geq \mathsf{tsl}_m$. Working in $F$ up to precision $N + nM$ we then calculate

$$\sum_{m=0}^{M} p^{-mn} \sum_{k=1}^{\mathsf{tsl}_m - 1}{}' b_k \tilde{z}^{kp^m},$$

where the prime indicates that we sum only over $k$ that are not divisible by $p$, $\tilde{z}$ is an approximation of $z$ up to precision $N + nM$ and $b_k$ is an approximation of $1/k^n$ up to the same precision.

(2) If $z$ is in $U_\infty$, then we calculate $(-1)^{n-1}\mathrm{Li}_n(1/z) - \log^n(z)/n!$. Here $\mathrm{Li}_n(1/z)$ is computed using (1), and it can be calculated up to precision $N$ if we know $z$ up to precision $\max\{N + nM + 2v_p(z), v_p(z)\}$ where $M$ is such that $-p^m v_p(z) - mn > N$ for all $m > M$. We can calculate $\log^n(z)/n!$ up to precision $N$ by first finding $V$ with $|\log(z)| \leq p^{-V}$ and knowing $z$ up to precision $N' > v_p(z)$ satisfying

$$\max\{V, N + v_p(n!) - (n-1)V\} \leq \min_{m \geq 0}\{(N' - v_p(z))p^m - m\}.$$

(3) If $z$ lies in $U_\zeta$ with $\zeta \neq 1$ in $F$ a root of unity of order dividing $p^f - 1$, then we proceed in several steps.

(a) We find $\mathsf{tsl} \geq 2$ such that $kv_p(z - \zeta) - n\log_p(k) > N$ for all $k \geq \mathsf{tsl}$.

(b) We find $\mathsf{gsl} \geq 2$ with the property that

$$\frac{k}{p-1} - \log_p(k) > N - m + c(m,p) + (n-m)\log_p(\mathsf{tsl} - 1)$$

for $m = 1, \ldots, n$ and all $k \geq \mathsf{gsl}$, where $c(m,p)$ is as in Proposition 6.1.

(c) We calculate the classes of $g_m(v)$ in $\mathbb{Q}_p[[v]]/(v^{\mathsf{gsl}})$ for $m = 1, \ldots, n$ inductively using Proposition 4.3, starting with the coefficients of $g_0(v)$ up to precision $N + n\log_p(\mathsf{tsl} - 1) + n\left\lfloor \log_p(\mathsf{gsl} - 1) \right\rfloor$.

(d) In $\mathbb{Q}_p(\zeta)$ we find an approximation $\tilde{\zeta}$ of $\zeta$ with $v_p(\tilde{\zeta} - \zeta) > N + n\log_p(\mathsf{tsl} - 1)$. Working in $\mathbb{Q}_p(\zeta)$ up to precision $N + n\log_p(\mathsf{tsl} - 1)$ we compute $\mathrm{Li}_m^{(p)}(\zeta^{p^j})$ for $j = 0, \ldots, f-1$ and $m = 1, \ldots, n$ up to precision $N - m + (n - m)\log_p(\mathsf{tsl} - 1)$ by evaluating the terms of degree smaller than $\mathsf{gsl}$ in $g_m(v)$ on $1/(1 - \tilde{\zeta}^{p^j})$.

(e) Still working in $\mathbb{Q}_p(\zeta)$ up to precision $N + n\log_p(\mathsf{tsl} - 1)$ we calculate $\mathrm{Li}_m(\zeta)$ up to precision $N + (n-m)\log_p(\mathsf{tsl} - 1)$ for $m = 1, \ldots, n$ by using Proposition 4.2, with the $\mathrm{Li}_m^{(p)}(\zeta^{p^j})$ $(j = 0, \ldots, f-1)$ replaced with the approximations obtained in (d).

(f) Working in $\mathbb{Q}_p(\zeta)[[t]]/(t^{\mathsf{tsl}})$ with coefficients up to precision $N + n\log_p(\mathsf{tsl} - 1)$ we use (4.5), (4.6) and (4.7), but with $\zeta$ replaced by $\tilde{\zeta}$ and the $\mathrm{Li}_m(\zeta)$ replaced by the approximations obtained in (e), in order to compute approximations to the terms of degree less than $\mathsf{tsl}$ in $F_{n,\zeta}(t)$.

(g) We then evaluate the terms of degree less than $\mathsf{tsl}$ in the result on $\tilde{z} - \tilde{\zeta}$ where $\tilde{z}$ is an approximation of $z$ of precision $N + n\log_p(\mathsf{tsl} - 1)$, and we work in $F$ up to precision $N + n\log_p(\mathsf{tsl} - 1)$.

(4) If $z \neq 1$ lies in $U_1$, then we calculate $\mathrm{Li}_n(z)$ up to precision $N$ by calculating both terms in (7.7) up to precision $N$, in several steps.

(a) We find $\mathsf{hsl} \geq 2$ such that $kv_p(z-1) > N + n\log_p(k)$ for all $k \geq \mathsf{hsl}$; if $p = 2$, then we increase $\mathsf{hsl}$ if necessary to ensure that $k > N - 1 + n\log_p(\mathsf{hsl} - 1)$ for all $k \geq \mathsf{hsl}$.

(b) If $p = 2$, then we compute the terms of degree less than $\mathsf{hsl}$ in

$$H_m(t) = b_{m,0} + b_{m,1}t + b_{m,2}t^2 + \cdots$$

for $m = 2, \ldots, n$ using (5.9) and (5.10), working in $\mathbb{Q}_2[[t]]/(t^{\mathsf{hsl}})$ up to precision $N + n\log_2(\mathsf{hsl} - 1)$ for the coefficients. At each stage we determine an approximation $\tilde{b}_{m,0}$ of $H_m(0) = b_{m,0}$, either as 0 if $m$ is even, or as $2^{m-1}(1-2^m)^{-1}\sum_{k=1}^{\mathsf{hsl}-1}\tilde{b}_{m,k}(-2)^k$ if $m$ is odd, where $\tilde{b}_{m,k}$ is the approximation of $b_{m,k}$.

If $p \neq 2$, then for $m = 2, \ldots, n$ we put $H_m(0) = 0$ when $m$ is even, and compute

$$H_m(0) = 2^{m-1}p^m g_m(1/2)/((1-2^{m-1})(p^m-1))$$

up to precision $N + (n-m)\log_p(\mathsf{hsl}-1)$ when $m$ is odd. For this we proceed as in (3)(b)–(d), using $\mathsf{gsl} \geq 2$ such that

$$\frac{k}{p-1} - \log_p(k) > N - m + c(m,p) + v_p(1-2^{m-1}) + (n-m)\log_p(\mathsf{hsl}-1)$$

for $k \geq \mathsf{gsl}$ and $m = 2, \ldots, n$, where $c(m,p)$ is as in Proposition 6.1, and we work up to precision

$$\max_{m=2,\ldots,n}\{N - m + v_p(1-2^{m-1}) + (n-m)\log_p(\mathsf{hsl}-1) + m\lfloor\log_p(\mathsf{gsl}-1)\rfloor\}$$

in $\mathbb{Q}_p$ for the coefficients of the $g_m(v)$'s ($m = 0, \ldots, n$). We then compute the terms of degree less than $\mathsf{hsl}$ in $H_n(t)$ by integration using (5.9) and (5.10), but with the $H_m(0)$ replaced by the approximations just obtained and working up to precision $N + n\log_p(\mathsf{hsl}-1)$ in $\mathbb{Q}_p$ for the coefficients.

(c) We find $V$ and $V_1$ with $V \leq v_p(\log(z))$ and $V_1 \leq v_p(\log(1-z))$ and put $\widetilde{N} = \max\{N + v_p((n-1)!), V_1 + (n-1)V\}$.

(d) We compute $\log^{n-1}(z)$ up to precision $\widetilde{N} - V_1$ as well as $-\log(1-z)$ up to precision $\widetilde{N} - (n-1)V$ and divide their product by $(n-1)!$. The calculation of $\log^{n-1}(z)$ up to the required precision can be done if we know $z$ up to precision $N' > 0$ satisfying

$$\max\{V, \widetilde{N} - V_1 - (n-2)V\} \leq \min_{m\geq 0}\{N'p^m - m\}\,.$$

The calculation of $-\log(1-z)$ can be done up to the required precision if we know $z$ up to precision $N'' > v_p(1-z)$ satisfying

$$\widetilde{N} - (n-1)V \leq \min_{m\geq 0}\{(N'' - v_p(1-z))p^m - m\}\,.$$

(e) Working in $F$ up to precision $N + n\log_p(\mathsf{hsl}-1)$ we evaluate the approximations of the terms of degree less than $\mathsf{hsl}$ in $H_n(t)$ as obtained in (b) on $\tilde{z}-1$ where $\tilde{z}$ is an approximation of $z$ of precision $N + n\log_p(\mathsf{hsl}-1)$. We add the result to the product obtained in (d), finding $\mathrm{Li}_n(z)$ up to precision $N$.

*Remark* 7.11. The conditions on $\mathsf{tsl}_m$, $\mathsf{tsl}$, $\mathsf{gsl}$ and $\mathsf{hsl}$ in (1), (3)(a), (3)(b), (4)(a) and (4)(b) of the algorithm are of the form $c_1 k - c_2 \ln(k) > c_3$ for all $k \geq \mathsf{tsl}_m$, etc., with positive $c_1$ and $c_2$. Since the left-hand side is increasing for $k > c_2/c_1$ it is very easy to find the minimum values for $\mathsf{tsl}_m$, etc.

We now justify the various steps in Algorithm 7.10. For (1) we use the next proposition.

**Proposition 7.12.** *Let $N > 0$ and let $z \neq 0$ be in $U_0$. If $M \geq 0$ is such that $p^m v_p(z) - mn > N$ for all $m > M$, $\tilde{z}$ is an approximation of $z$ up to precision $N + nM$, and for $m = 0, \ldots, M$ we choose $\mathsf{tsl}_m > 0$ such that $kp^m v_p(z) - mn > N$ for $k \geq \mathsf{tsl}_m$, then*

$$\sum_{m=0}^{M} p^{-mn} {\sum_{k=1}^{\mathsf{tsl}_m - 1}}' \frac{\tilde{z}^{kp^m}}{k^n},$$

*where the prime indicates that we sum only over $k$ that are not divisible by $p$, is an approximation of $\mathrm{Li}_n(z)$ up to precision $N$. Moreover, we can replace each $1/k^n$ by an approximation up to precision $N + nM$.*

*Proof.* It is clear from (3.3) that $|\mathrm{Li}_n^{(p)}(z)| = |z|$ when $|z| < 1$. Therefore, from (3.4) we see that in order to compute $\mathrm{Li}_n(z)$ up to precision $N$ we only have to compute $\sum_{m=0}^{M} p^{-mn} \mathrm{Li}_n^{(p)}(z^{p^m})$ if $p^m v_p(z) - mn > N$ for all $m > M$. So we reduce to the calculation of $p^{-mn}\mathrm{Li}_n^{(p)}(z^{p^m})$ up to precision $N$ for $m = 0, \ldots, M$. In the corresponding power series $p^{-mn} {\sum_{k=1}^{\infty}}' z^{kp^m}/k^n$ we can ignore terms with valuation bigger than $N$, i.e., where $kp^m v_p(z) - mn > N$.

Finally, for each term $p^{-mn} z^{kp^m}/k^n$ that we compute we can replace $z$ with an approximation $\tilde{z}$ satisfying $v_p(z - \tilde{z}) > N + mn$ and $1/k^n$ with an approximation $b_k$ satisfying $v_p(1/k^n - b_k) > N + mn$, and obtain that term up to precision $N$. This follows from the identity $z^{kp^m}/k^n - b_k \tilde{z}^{kp^m} = (z^{kp^m} - \tilde{z}^{kp^m})/k^n + (1/k^n - b_k)\tilde{z}^{kp^m}$ since $v_p(k^n) = 0$, and $v_p(z) > 0$ implies that $v_p(z^{kp^m} - \tilde{z}^{kp^m}) \geq v_p(z - \tilde{z})$ and $v_p(\tilde{z}^{kp^m}) > 0$. □

In (2) we use the fact that $\mathrm{Li}_n(z) = (-1)^{n-1}\mathrm{Li}_n(1/z) - \log^n(z)/n!$ by Proposition 2.10(2). For the term $\mathrm{Li}_n(1/z)$ we use (1), and the corresponding precision of $z$ also follows from this part together with Remark 7.2(4) because we are assuming that we know $z$ up to positive relative precision. The term $-\log^n(z)/n!$ can be readily calculated using standard methods, so we only give estimates for the precision of $z$ that enables us to calculate it up to precision $N$.

**Lemma 7.13.** *If $y$ in $\mathbb{C}_p$ satisfies $|y| \leq p^{-V}$ and is known up to precision $N' \geq V$, then $y^n$ for $n \geq 1$ is known up to precision $N' + (n-1)V$.*

*Proof.* By assumption we know $y + \varepsilon$ for some $\varepsilon$ in $\mathbb{C}_p$ with $|\varepsilon| < p^{-N'}$. Then $|(y+\varepsilon)^n - y^n| = |\varepsilon| \cdot |y^{n-1} + \varepsilon y^{n-2} + \cdots + \varepsilon^{n-2} y + \varepsilon^{n-1}| < p^{-N'} p^{-(n-1)V}$ because $N' \geq V$. □

As for the logarithm we have the following result.

**Lemma 7.14.** *If we know $z$ in $\mathbb{C}_p^*$ up to precision $N' > v_p(z)$, then we can calculate $\log(z)$ up to precision $\min_{m \geq 0}\{(N' - v_p(z))p^m - m\}$. If $1 \leq (N' - v_p(z))\ln(p)$, then we can calculate $\log(z)$ up to precision $N' - v_p(z)$.*

*Proof.* Since we know $z$ up to precision $N'$ we know $\tilde{z} = z + \varepsilon$ with $|\varepsilon| < p^{-N'}$. Then $\log(\tilde{z}) - \log(z) = \log(1+\varepsilon/z) = -\mathrm{Li}_1(-\varepsilon/z)$. Since $v_p(\varepsilon/z) > N' - v_p(z) > 0$ the estimates in Remark 7.5 apply. □

The last inequality in part (2) of the algorithm is then justified by the next proposition. Note that Lemma 7.14 in practice allows us to bound $|\log(z)|$, as is required here. (But see also Remark 8.1.)

**Proposition 7.15.** *If, for $z$ in $\mathbb{C}_p^*$, $|\log(z)| \leq p^{-V}$ and we know $z$ up to precision $N' > v_p(z)$ satisfying*

$$\max\{V, N + v_p(n!) - (n-1)V\} \leq \min_{m\geq 0}\{(N' - v_p(z))p^m - m\},$$

*then we can compute $\log^n(z)/n!$ up to precision $N$.*

*Proof.* It suffices to calculate $\log^n(z)$ up to precision $N + v_p(n!)$. By Lemma 7.13 we can do this if we know $\log(z)$ up to precision $N'' = \max\{V, N + v_p(n!) - (n-1)V\}$. In order to compute $\log(z)$ up to precision $N''$, it suffices by Lemma 7.14 to know $z$ up to precision $N' > v_p(z)$ satisfying $\min_{m\geq 0}\{(N' - v_p(z))p^m - m\} \geq N''$. □

For step (3) of the algorithm we need some more results.

**Proposition 7.16.** *Let $g_n(v)$ be as in Proposition 4.3, and let $c(n,k)$ be as in Proposition 6.1. To compute $g_n(\alpha)$ up to precision $N' > 0$ when $v_p(\alpha) = 0$ it suffices to know $\alpha$ up to precision $N'$ and to evaluate the sum of the terms in $g_n(v)$ of degree less than $\mathsf{gsl}'$ on the approximation of $\alpha$, where $\mathsf{gsl}'$ is such that $\frac{k}{p-1} - \log_p(k) - c(n,p) > N'$ for all $k \geq \mathsf{gsl}'$. In fact, it suffices to use approximations up to precision $N'$ for the coefficients of the terms of degree less than $\mathsf{gsl}'$.*

*Similarly, in order to know $\mathrm{Li}_n^{(p)}(\zeta)$ up to precision $N' > 0$ for a root of unity $\zeta \neq 1$ of order not divisible by $p$, it suffices to know $\zeta$ and the coefficients of the terms of $g_n(v)$ of degree less than $\mathsf{gsl}'$ up to precision $N'$, where $\mathsf{gsl}'$ is as before.*

*Proof.* The first statement follows from the estimates for the valuations of the coefficients of $g_n(v)$ as given in Proposition 6.1. It implies the second because $v_p(1/(1-\zeta)) = 0$, $\mathrm{Li}_n^{(p)}(\zeta) = g_n(1/(1-\zeta))$, and $1/(1-\zeta)$ is known to the same precision as $\zeta$ by Remark 7.2(4). □

*Remark* 7.17. Computing the coefficients of $g_n(v)$ as rational numbers is very inefficient so, instead, we use coefficients in $\mathbb{Q}_p$ with finite precision. If $g_n(v) = a_{n,1}v + a_{n,2}v^2 + \cdots$, then $ka_{n+1,k} = -(a_{n,1} + a_{n,2} + \cdots + a_{n,k})$ by Proposition 4.3. Hence, if we know $a_{n,k}$ for $1 \leq k \leq \mathsf{gsl}' - 1$ up to precision $\widetilde{N}$, then we know $a_{n+1,k}$ for $1 \leq k \leq \mathsf{gsl}' - 1$ up to precision $\widetilde{N} - \lfloor \log_p(\mathsf{gsl}' - 1) \rfloor$. In particular, using the method of Proposition 4.3 we can compute $a_{n,k}$ for $k = 1, \ldots, \mathsf{gsl}' - 1$ up to precision $N'$ if we know $a_{0,k}$ for $k = 1, \ldots, \mathsf{gsl}' - 1$ up to precision $N' + n\lfloor \log_p(\mathsf{gsl}' - 1) \rfloor$.

For the power series $F_{n,\zeta}(t)$ instead of $g_n(v)$, where $\zeta \neq 1$ is a $(p^f - 1)$-th root of unity, the corresponding statements in the next proposition are more involved.

**Proposition 7.18.** *Assume that $z$ lies in the residue disc $U_\zeta$ for $\zeta \neq 1$ a $(p^f - 1)$-th root of unity and let*

$$F_{n,\zeta}(t) = a_{n,0} + a_{n,1}t + a_{n,2}t^2 + \cdots$$

*be the Taylor expansion of $\mathrm{Li}_n(z)$ around $\zeta$ as in Proposition 4.4. Let $\mathsf{tsl}' > 0$ be such that $v_p(a_{n,k}(z-\zeta)^k) > N$ for all $k \geq \mathsf{tsl}'$ and assume that the $\mathrm{Li}_m(\zeta)$ for*

*$m = 1, \dots, n$ are known up to precision $N + (n-m)\log_p(\mathsf{tsl}' - 1)$. If $\zeta$ and $z$ are known up to precision $N + n\log_p(\mathsf{tsl}' - 1)$, then we can compute $\mathrm{Li}_n(z)$ up to precision $N$ by:*

1. *finding the terms of degree less than $\mathsf{tsl}'$ in $F_{0,\zeta}(t)$ as in (4.5) with $\zeta$ replaced with its approximation;*
2. *for $m = 1, \dots, n$ computing the terms of degree less than $\mathsf{tsl}'$ in $F_{m,\zeta}(t)$ up to precision $N + (n-m)\log_p(\mathsf{tsl}' - 1)$ via repeated integration of (4.6), using the approximate values for $\zeta$ and $F_{m,\zeta}(0) = \mathrm{Li}_m(\zeta)$;*
3. *evaluating the terms of degree less than $\mathsf{tsl}'$ in the approximation of $F_{n,\zeta}(t)$ on the difference of the approximations of $z$ and $\zeta$.*

*Proof.* Note that $\mathsf{tsl}'$ as in the statement of the proposition exists by Proposition 6.7 or Remark 6.9. We can therefore compute $\mathrm{Li}_n(z)$ up to precision $N$ by computing $a_{n,0} + a_{n,1}(z-\zeta) + \cdots + a_{n,\mathsf{tsl}'-1}(z-\zeta)^{\mathsf{tsl}'-1}$. Using an approximation $\tilde{\zeta}$ of $\zeta$ in (4.5) we have an approximation

$$\widetilde{F}_{m,\zeta}(t) = \tilde{a}_{m,0} + \tilde{a}_{m,1}t + \cdots$$

of $F_{m,\zeta}(t)$ for $m = 0$. We use $\widetilde{F}_{m,\zeta}(t)$ instead of $F_{m,\zeta}(t)$ and $\tilde{\zeta}$ instead of $\zeta$ in (4.6) in order to inductively obtain an approximation

$$\widetilde{F}_{m+1,\zeta}(t) = \tilde{a}_{m+1,0} + \tilde{a}_{m+1,1}t + \cdots$$

of $F_{m+1,\zeta}(t)$. Here $k\tilde{a}_{m+1,k} = -\sum_{j=0}^{k-1}(-\tilde{\zeta})^{j-k}\tilde{a}_{m,j}$ for $k = 1, 2, \dots, \mathsf{tsl}' - 1$, as in (6.8). Inductively we may assume that $v_p(\tilde{a}_{m,j} - a_{m,j}) > N + (n-m)\log_p(\mathsf{tsl}' - 1)$ for $j = 0, \dots, \mathsf{tsl}' - 1$ since this holds for $m = 0$ by our assumption on $v_p(\tilde{\zeta} - \zeta)$, Remark 7.2(4) and (4.5). Then for $k = 1, \dots, \mathsf{tsl}' - 1$ we have, as in the proof of Proposition 6.7,

$$\begin{aligned} k(a_{m+1,k} - \tilde{a}_{m+1,k}) &= \sum_{j=0}^{k-1}\left((-\tilde{\zeta})^{j-k}\tilde{a}_{m,j} - (-\zeta)^{j-k}a_{m,j}\right) \\ &= \sum_{j=0}^{k-1}(-1)^{j-k}\left[\tilde{\zeta}^{j-k}(\tilde{a}_{m,j} - a_{m,j}) + (\tilde{\zeta}^{j-k} - \zeta^{j-k})a_{m,j}\right]. \end{aligned}$$

Since $v_p(\tilde{\zeta}^{j-k}) \geq 0$ and $v_p(\tilde{\zeta}^{j-k} - \zeta^{j-k}) > N + n\log_p(\mathsf{tsl}' - 1)$ by our assumptions, by Proposition 6.7 it follows as in the proof of that proposition that

$$v_p(\tilde{a}_{m+1,k} - a_{m+1,k}) > N + (n - (m+1))\log_p(\mathsf{tsl}' - 1)$$

for $k = 1, \dots, \mathsf{tsl}' - 1$. Finally, $v_p(\tilde{a}_{m+1,0} - a_{m+1,0}) > N + (n-(m+1))\log_p(\mathsf{tsl}' - 1)$ since we assume that we have such an approximation $\tilde{a}_{m+1,0}$ for $a_{m+1,0} = \mathrm{Li}_{m+1}(\zeta)$.

Now we consider the terms $a_{n,j}(z-\zeta)^j$ for $j = 0, \dots, \mathsf{tsl}' - 1$. For $j = 0$ we have $v_p(a_{n,0} - \tilde{a}_{n,0}) > N$ by assumption. For $j > 0$ this term is approximated by $\tilde{a}_{n,j}(\tilde{z} - \tilde{\zeta})^j$ with $\tilde{z}$ an approximation of $z$ up to precision $N + n\log_p(\mathsf{tsl}' - 1)$ and

$$a_{n,j}(z-\zeta)^j - \tilde{a}_{n,j}(\tilde{z} - \tilde{\zeta})^j = (a_{n,j} - \tilde{a}_{n,j})(z-\zeta)^j + \tilde{a}_{n,j}((z-\zeta)^j - (\tilde{z} - \tilde{\zeta})^j).$$

We have just seen that $v_p(a_{n,j} - \tilde{a}_{n,j}) > N$, and since $v_p(z-\zeta) > 0$ by assumption the first term in the right-hand side has valuation bigger than $N$. The second term has valuation at least $v_p(\tilde{a}_{n,j}) + v_p((z-\zeta) - (\tilde{z} - \tilde{\zeta}))$. Proposition 6.7 implies that $v_p(\tilde{a}_{n,j}) \geq \min\{v_p(a_{n,j} - \tilde{a}_{n,j}), v_p(a_{n,j})\} \geq -n\log_p(\mathsf{tsl}' - 1)$, so the valuation of the second term is bigger than $N$ by our assumptions on $v_p(z - \tilde{z})$ and $v_p(\zeta - \tilde{\zeta})$. □

We can now justify Algorithm 7.10(3). Remark 7.17 implies that (c) computes the coefficients of the terms of degree less than $\mathsf{gsl}$ in $g_m(v)$ $(m = 1, \dots, n)$ up to precision $N + n\log_p(\mathsf{tsl} - 1) + (n - m)\lfloor \log_p(\mathsf{gsl} - 1)\rfloor$. In (d), for $m = 1, \dots, n$ let $N'_m = N - m + (n-m)\log_p(\mathsf{tsl}-1)$. If $N'_m > 0$, then the indicated method calculates $\mathrm{Li}_m^{(p)}(\zeta^{p^j}) = g_m(1/(1-\zeta^{p^j}))$ up to precision $N'_m$ by Proposition 7.16: $v_p(\tilde{\zeta} - \zeta) > N'_m$ so according to Remark 7.2(4) we have $v_p(1/(1-\tilde{\zeta}^{p^j}) - 1/(1-\zeta^{p^j})) > N'_m$; $k/(p-1) - \log_p(k) - c(m,k) > N'_m$ for all $k \geq \mathsf{gsl}$ by (b); and the relevant coefficients in $g_m(v)$ are known up to precision $N'_m$ from (c). If $N'_m \leq 0$, then we observe that the valuation of the difference between what we calculate in (d) and $g_m(1/(1-\zeta^{p^j}))$ is bigger than $N'_m$ by Proposition 6.1 since $v_p(1/(1-\tilde{\zeta}^{p^j}) - 1/(1-\zeta^{p^j})) > 0$ and $k/(p-1) - \log_p(k) - c(m,p) > N'_m$ for $k \geq \mathsf{gsl}$ by (b). (Note that we always know the coefficients of $g_m(v)$ that we compute up to precision $N'_m$.) Now (e) is immediate from (d), taking into account the valuations of the coefficients of the various contributions to $\mathrm{Li}_m(\zeta^{p^j})$ when applying Proposition 4.2. Finally, (f) and (g) then follow from Proposition 7.18 together with its proof by our choice of $\mathsf{tsl}$ in (a) since $v_p(a_{n,k}) \geq -n\log_p(k)$ by Proposition 6.7.

We conclude this section by justifying Algorithm 7.10(4), dealing first with the term $-\log^{n-1}(z)\log(1-z)/(n-1)!$ in (7.7), i.e., steps (c) and (d).

If for some $\alpha$ and $\beta$ in $\mathbb{C}_p$ we have $V_\alpha \leq v_p(\alpha)$ and $V_\beta \leq v_p(\beta)$, then for the calculation of $\alpha\beta$ up to precision $N$ it suffices to compute $\alpha$ up to precision $N - V_\beta$ and $\beta$ up to precision $N - V_\alpha$, at least if $N - V_\alpha - V_\beta \geq 0$. By increasing $N$ if necessary we may always assume the latter. For $z \neq 1$ in $U_1$ we let $\alpha = \log^{n-1}(z)$, $\beta = -\log(1-z)$ and replace $N$ with $N + v_p((n-1)!)$. Using Lemma 7.14 we find $V$ and $V_1$ with $V \leq v_p(\log(z))$ and $V_1 \leq v_p(\log(1-z))$. Then we let

$$\widetilde{N} = \max\{N + v_p((n-1)!), V_1 + (n-1)V\}$$

and compute $\log^{n-1}(z)$ up to precision $\widetilde{N} - V_1$ as well as $-\log(1-z)$ up to precision $\widetilde{N} - (n-1)V$. We can do this by applying Proposition 7.15 and Lemma 7.14, taking into account that $v_p(z) = 0$. This together with the estimates above gives (4)(c)–(d) of Algorithm 7.10.

For the computation of $H_n(z-1)$ up to precision $N$, which corresponds to the remaining steps of (4), we use the following result and, if $p = 2$, also Proposition 7.20.

**Proposition 7.19.** *Assume $z$ is in the residue disc $U_1$ and, for $n \geq 2$, let*

$$H_n(t) = b_{n,0} + b_{n,1}t + b_{n,2}t^2 + \cdots$$

*be as in Propositions 5.8 and 6.11. Let $\mathsf{hsl}' > 0$ be such that $v_p(b_{n,k}(z-1)^k) > N$ for all $k \geq \mathsf{hsl}'$ and assume that $H_m(0)$ for $m = 2, \dots, n$ is known up to precision $N + (n-m)\log_p(\mathsf{hsl}'-1)$. If $z$ with $|z| < 1$ is known up to precision $N + n\log_p(\mathsf{hsl}'-1)$, then we can compute $H_n(z-1)$ up to precision $N$ by:*

1. *finding the terms of degree less than $\mathsf{hsl}'$ of $G_2(t)$ and $H_2(t)$ with coefficients up to precision $N + (n-2)\log_p(\mathsf{hsl}' - 1)$;*
2. *for $m = 3, \dots, n$ computing the terms of degree less than $\mathsf{hsl}'$ in $G_m(t)$ and $H_m(t)$ up to precision $N + (n-m)\log_p(\mathsf{hsl}' - 1)$ via repeated integration of $G'_n(t) = G_{n-1}(t)/(1+t)$ and (5.10), using $G_m(0) = 0$ and the approximate values for $H_m(0)$;*
3. *evaluating the terms of degree less than $\mathsf{hsl}'$ in the approximation of $H_n(t)$ on the difference of the approximation of $z$ and 1.*

*Proof.* Parts (1) and (2) are proved as in the proof of Proposition 7.18 by induction on $m$ starting with $m = 2$, but for $G_m(t)$ and $H_m(t)$ simultaneously and with the simplification that we do not have to approximate 1. The estimate for (3) also goes as in that proof, the estimates for the coefficients of $H_n(t)$ in Proposition 6.11 being the same as for those of $F_{n,\zeta}(t)$ in Proposition 6.7. □

In order to apply this proposition we need to determine $H_m(0)$ up to precision $N + (n-m)\log_p(\mathsf{hsl}' - 1)$ for $m = 2, \dots, n$, and, according to Remark 5.12(1), only for $m$ odd.

When $p \neq 2$ we have $H_m(0) = 2^{m-1}p^m \mathrm{Li}_m^{(p)}(-1)/((1-2^{m-1})(p^m-1))$ by Remark 5.12(2), so we only have to calculate $\mathrm{Li}_m^{(p)}(-1)$ up to precision

$$N + (n-m)\log_p(\mathsf{hsl}' - 1) + v_p(1-2^{m-1}) - m$$

for $m$ odd with $2 \leq m \leq n$. In Algorithm 7.10(4)(b) we have done this along the lines of (3)(b)–(d) of the algorithm. The justification for this is similar to the one given after Proposition 7.18, putting

$$N'_m = N - m + v_p(1-2^{m-1}) + (n-m)\log_p(\mathsf{hsl} - 1),$$

but with the simplification that $\zeta = -1$ is now known exactly, and using Proposition 6.11 instead of Proposition 6.7. Step (4)(e) is then immediate from the last part of Proposition 7.19.

When $p = 2$ we use (5.11) in order to compute $H_m(0)$, and for this we formulate a supplement to Proposition 7.19. Note that we can always attain the condition on $\mathsf{hsl}'$ below by increasing it if necessary, as stated in (4)(a) of the algorithm.

**Proposition 7.20.** *Let $p = 2$ and assume that $\mathsf{hsl}'$ in Proposition 7.19 also satisfies*

$$k + v_p(b_{m,k}) > N - (m-1) + (n-m)\log_p(\mathsf{hsl}' - 1)$$

*for all $k \geq \mathsf{hsl}'$ and all $m = 2, \dots, n$. Then in the inductive procedure of Proposition 7.19 we can calculate $H_m(0)$ for $m = 2, \dots, n$ up to the required precision as $2^{m-1}(1-2^m)^{-1}\sum_{k=1}^{\mathsf{hsl}'-1}\tilde{b}_{m,k}$ where $\tilde{b}_{m,k}$ is the approximation of $b_{m,k}$.*

*Proof.* We know from (5.11) that $H_m(0) = 2^{m-1}(H_m(-2) - H_m(0))/(1-2^m)$. The extra condition on $\mathsf{hsl}'$ means that for $m = 2, \dots, n$ we can compute $H_m(-2) - H_m(0)$ up to precision $N - (m-1) + (n-m)\log_p(\mathsf{hsl}' - 1)$ using the non-constant terms of degree less than $\mathsf{hsl}'$ in $H_m(t)$. Inductively

$$v_p(\tilde{b}_{m,k} - b_{m,k}) > N + (n-m)\log_p(\mathsf{hsl}' - 1)$$

for $k = 1, \dots, \mathsf{hsl}' - 1$, so that

$$H_m(-2) - H_m(0) - \sum_{k=1}^{\mathsf{hsl}'-1} \tilde{b}_{m,k}(-2)^k$$

has valuation at least $N - (m-1) + (n-m)\log_p(\mathsf{hsl}' - 1)$. So the formula in the proposition approximates $H_m(0)$ up to precision $N + (n-m)\log_p(\mathsf{hsl}' - 1)$. □

Now Algorithm 7.10(4)(a), (b) and (e) for $p = 2$ follow from Propositions 7.19 and 7.20 combined with Proposition 6.11.

This finishes the justification of Algorithm 7.10.

## 8. Concluding remarks

In this section we describe how to make the estimates in it uniform for all elements in a fixed finite extension of $\mathbb{Q}_p$, analyze the corresponding asymptotic time and make a remark about an alternative approach for computing the constant term of the $F_{n,\zeta}(t)$.

*Remark* 8.1. In case one wants to compute $\mathrm{Li}_n(z)$ for several $z$ in a field $F$ with finite ramification index $e$ over $\mathbb{Q}_p$ it is probably more efficient to compute the (approximations of the truncated) power series in Algorithm 7.10 as they are needed using universal estimates and to remember them.

Namely, if $z$ lies in the residue disc $U_a$ with $a \neq \infty$, then $v_p(z-a) \geq 1/e$. For $\log(z)$ with $z$ in $F^*$ we observe that $v_p(\log(z)) \geq \min\{v_p(\log(p)), v_p(\log(y))\} - v_p(e)$ for some $y$ in $U_1$ because we can take $b = e$ in Remark 2.2 and $\log(\eta) = 0$ for any root of unity $\eta$. Then $y = 1+x$ with $v_p(x) \geq 1/e$ and, for $m \geq 0$, $y^{p^m} = (1+x)^{p^m} = 1+x'$ with

$$v_p(x') \geq \min\{m + 1/e, (m-1) + p/e, \ldots, 1 + p^{m-1}/e, p^m/e\}$$

as one easily sees by induction on $m$. If we choose $m \geq 0$ such that this minimum is at least $1/(p-1)$, i.e., such that $p^m \geq e/(p-1)$, then $v_p(p^m \log(1+x)) = v_p(\log(1+x')) \geq v_p(x') \geq 1/(p-1)$ by [16, Lemma 5.5]. Therefore $v_p(\log(z)) \geq \min\{v_p(\log(p)), 1/(p-1) - m\} - v_p(e)$ for all $z$ in $F^*$.

Using those bounds one can obtain, in each of the four cases in the algorithm, universal estimates for the lengths of the power series involved, etc., or the precision required for $z$. However, for the computation of $\log(z)$ or its powers up to a given precision in (2) the estimates involve the relative precision of $z$. The same applies to $1-z$ when we calculate $\log(1-z)$ in (4)(d).

We conclude by analyzing the time needed by the algorithm. For simplicity we only deal with the main case, that is of elements $z$ satisfying $|z| = |z-1| = 1$, treated in part (3) of the algorithm. We recall the $O^\sim$ notation (see for example [15]), where being $O^\sim(x)$ means being $O(x \ln^c(x))$ for some constant $c$.

**Theorem 8.2.** *Suppose that $z$ satisfies $|z| = |z-1| = 1$ and belongs to a fixed finite extension $F$ of $\mathbb{Q}_p$ with ramification index $e$ and residue extension degree $f$. Then Algorithm 7.10 computes $\mathrm{Li}_n(z)$ up to precision $N$ with*

$$O^\sim(N^2 f(fnp + ne\ln(p) + e^2\ln(p)))$$

*additions and multiplications and $O^\sim(p)$ divisions, provided that $2n\log_p(N) < N$, $2n\log_p(2e) < N$ and $2p\log_p(N) < N$.*

*Proof.* We assume that $F$ is given explicitly as a purely ramified extension of degree $e$ of an unramified extension $F^{\mathrm{unr}}$ of $\mathbb{Q}_p$ of degree $f$. We begin by describing basic operations in $\mathbb{Q}_p$, $F^{\mathrm{unr}}$, $F$ and polynomial rings above these fields, as applied in our algorithm. One first of all observes that we can always work in the rings of integers of these fields: in step (c) the coefficients are always in $\mathbb{Z}_p$ by Proposition 6.1, while in steps (f) and (g) the coefficients are in $F^{\mathrm{unr}}$ but have bounded denominators by Proposition 6.7, and it is possible to multiply first by a fixed power of $p$ to eliminate these denominators and divide out this power in the end. Working with $\mathbb{Z}_p$ up to a fixed precision $k$ means working in $\mathbb{Z}/p^k$. Arithmetic operations modulo powers of 2 are easily done on a computer by ignoring most significant bits, so let us suppose

that $p \neq 2$. Then we can avoid doing divisions in these computations by using Montgomery arithmetic [12].

Recall that in Montgomery arithmetic one represents a number $x$ in $\mathbb{Z}/p^k$ by its so called Montgomery representative $x_M := Rx \pmod{p^k}$, where $R$ is a power of $2^t$, with $t$ the length of a computer word in bits, such that $R > p^k$. Operations in $\mathbb{Z}/p^k$ are replaced by equivalent operations on representatives, the main benefit being that multiplication can be done without using division with remainder, costing a fixed multiple of the cost of integer multiplication instead, and with no additional cost for the other operations.

If $x$ is known to be divisible by $p$, then so is $x_M$ and $(x/p)_M = x_M/p$. Furthermore, in this case we can compute $x_M/p$ as $x_M \cdot p^{-1} \pmod{R}$, where $p^{-1}$ is a precomputed inverse modulo $R$. Thus, no divisions are required. In general, dividing by $p^j u$, where $u$ is invertible, requires the computation of the inverse of $u$ modulo $p$, for which a gcd algorithm is used, and then a Newton iteration method to lift this to an inverse of $u$ modulo $p^k$. We may precompute the inverses of all elements modulo $p$, and even the most naive algorithm for this will only require $O^{\sim}(p)$ divisions. We may in fact notice that the only divisions that are actually carried out during the algorithm are by integers in the range from 2 to $\max(\mathsf{tsl}, \mathsf{gsl})$. Thus, it is reasonable to simply precompute once the inverses of all of these integers. After this has been done operations in $\mathbb{Z}_p$ to precision $k$ cost a fixed multiple of the same operation in $\mathbb{Z}$ with integers which are of size at most $p^k$, and its complexity is $O^{\sim}(k \ln(p))$ additions and multiplications for multiplication if fast integer multiplication [15, Theorem 8.24] is used. Addition is clearly faster.

We must also take into account the cost of the conversion from and to Montgomery representatives. The former is smaller than a single multiplication and has to be done only at the very end. The latter involves a division by $p^k$. Since $z$ is initially represented as a polynomial of degree $ef$ with $\mathbb{Z}/p^k$ coefficients, we will have to convert to Montgomery form all of these coefficients. We further have to convert 1. Other elements that may appear in the algorithm are derived from these. We need certain roots of unity in the algorithm, but for their computation we use $z$ as a starting point for Newton iterations. We also need certain integers when computing the coefficients of the power series we are working with. These are easily seen to be consecutive integers (for example denominators one obtains when integrating power series), so we will get them by successively adding 1's in the Montgomery representation. To eliminate divisions in the conversion we may observe that division with remainder by $p^k$ may be replaced by multiplication by a precomputed $R'/p^k$, where $R'$, again a power of $2^t$, should be bigger than all the possible $Rx$ (say $R' = R^2$), followed by division by $R'$ (shifting by a number of computer words). The amount of multiplications required here is negligible compared with the overall complexity (we neglect the complexity of the computation of $R'/p^k$, which has to be done only once for each $p$ and fixed precision). The conclusion is that conversion to and from Montgomery representatives does not add to the overall complexity.

Next we describe arithmetic in $\mathcal{O}_{F^{\mathrm{unr}}}$ and $\mathcal{O}_F$, the valuation rings of $F^{\mathrm{unr}}$ and $F$. These rings can be realized as extensions of the form $\mathbb{Z}_p[x]/(g)$, with $g$ an appropriate polynomial. By using polynomial Montgomery arithmetic (this is described for

polynomials over fields in [11] but can trivially be adapted to other rings as well) we are again reduced to additions and multiplications of degree at most $\deg(g)$. We can use FFT multiplication to do this with $O^\sim(\deg g)$ additions and multiplications in $\mathbb{Z}_p$ [15, Theorem 8.23].

This completes the estimate of the complexity of the basic operations. Let us summarize this as follows. We have to do three types of multiplications, whose complexity estimates for precision $x$ are as follows:

- multiplications in $\mathbb{Q}_p$, which take $O^\sim(x\ln(p))$,
- multiplications in $F^{\mathrm{unr}}$, which take $O^\sim(xf\ln(p))$,
- multiplications in $F$, which take $O^\sim(xfe\ln(p))$

where all numbers count additions and multiplications. Now let us consider each of the steps in Algorithm 7.10(3).

(a) By its definition and Remark 8.1 we have $\mathsf{tsl} = O(Ne)$. Here we are using our assumptions on the size differences between $N$, $n$ and $e$. Indeed, we have to guarantee that $k/e - n\log_p(k) > N$ for all $k > \mathsf{tsl}$. We shall show that we can take $\mathsf{tsl} = 2Ne$. Since the function $k/e - n\log_p(k)$ is increasing from $2Ne$ onward provided $2N\ln(p) \geq n$, which is guaranteed by our conditions, we only need to make sure that $n\log_p(2Ne) < N$. But this is true by the first two of our conditions, which can be rewritten as $N - n\log_p(N) > N/2 > n\log_p(2e)$.

(b) Here we have $\mathsf{gsl} = O(pN)$, again using our conditions.

(c) Now we have to compute the expansion of the $g_m(v)$'s to $\mathsf{gsl}$ places. There are $n$ steps, each consisting of a polynomial multiplication of length $O(pN)$ with the coefficients up to precision $N$. Note that this computation is done in $\mathbb{Q}_p$. It is done in time $O^\sim(n \cdot pN \cdot N\ln(p)) = O^\sim(npN^2)$.

(d1) We find $\tilde{\zeta}$ in $F^{\mathrm{unr}}$ by using Newton's method to solve $x^{p^f-1} = 1$. As the required precision is $O(N)$, under our assumptions the algorithm will be about $\ln(N)$ steps, each consisting of about $\ln(p^f) = f\ln(p)$ multiplications which are carried out again to precision $N$ in $F^{\mathrm{unr}}$. The total complexity is $O^\sim(\ln(N) \cdot f\ln(p) \cdot Nf\ln(p)) = O^\sim(Nf^2\ln^2(p))$.

(d2) Each of the $g_m(v)$ has to be evaluated at $f$ elements derived from powers of the $\tilde{\zeta}$. This is done in $F^{\mathrm{unr}}$. As the precision is $O(N)$ and the polynomials are of length $O(pN)$, the complexity is $O^\sim(n \cdot f \cdot Np \cdot Nf\ln(p)) = O^\sim(np(Nf)^2)$.

(e) For the calculation of $\mathrm{Li}_m(\zeta)$ for all $m \leq n$ we evaluate the expression in Proposition 4.2 of length $f$, which involves an addition and multiplication in $F^{\mathrm{unr}}$, and powers of $p$. The total time for this is $O^\sim(n \cdot f \cdot Nf\ln(p)) = O^\sim(nf^2N\ln(p))$ since there are no denominators involved and, taking $\mathsf{tsl} = 2Ne$ as before, the required precision is $O(N)$ by our assumptions.

(f) The computation of $F_{n,\zeta}(t)$ involves $n$ times multiplication of polynomials of degree $O(Ne)$ with coefficients in $F^{\mathrm{unr}}$, hence takes time

$$O^\sim(n \cdot Ne \cdot Nf\ln(p)) = O^\sim(nfeN^2\ln(p)).$$

Note that we used the fact that we can work with polynomials with coefficients in $\mathcal{O}_{F^{\mathrm{unr}}}$ by multiplying by $p^N$ by Proposition 6.7 and our assumptions, dividing out this power of $p$ and the end. The resulting precision needed in $\mathcal{O}_{F^{\mathrm{unr}}}$ is at most $3N$ under our assumptions.

(g) This step consists of evaluating a polynomial of degree $O(Ne)$ at an element of $\mathcal{O}_F$, so it takes time $O^{\sim}(Ne \cdot Nfe\ln(p)) = O^{\sim}(f(Ne)^2\ln(p))$. Again we used the fact that the relevant coefficients of $p^N F_{n,\zeta}(t)$ lie in $\mathcal{O}_{F^{\mathrm{unr}}} \subseteq \mathcal{O}_F$.

Looking at the time complexities of all the steps we see that those of (d2), (f) and (g) dominate, and their sum gives our time estimate. □

*Remark* 8.3. (1) The estimates in Theorem 8.2 are based on computing the value at $z$ from scratch. As mentioned in Remark 8.1, if we want to compute $\mathrm{Li}_n(z)$ for several $z$ in the same residue disc $U_\zeta$, then it is more efficient to compute the approximation of the truncation of $F_{n,\zeta}(t)$ and remember it, since then only (g) will have to be performed again.

(2) The time estimates in Theorem 8.2 are worst case estimates. If $z$ is closer to the root of unity $\zeta$ the complexities of (f) and (g) are reduced, since one needs fewer terms in the power series expansion around $\zeta$ to achieve the required precision.

**Example 8.4.** Tables 1 through 4 give the cpu times (in seconds) taken by the calculation of $\mathrm{Li}_n(z)$ up to precision $N$ using Algorithm 7.10, for various $F$, $N$, $n$, $p$ and $z$. In all cases we used $F = \mathbb{Q}_p(\zeta, \pi)$ with $\zeta \neq 1$ a primitive $(p^f - 1)$-th root of unity and $\pi$ a root of the Eisenstein polynomial $q(x)$. So $F^{\mathrm{unr}} = \mathbb{Q}_p(\zeta)$ is the unramified extension of $\mathbb{Q}_p$ of degree $f$, $F = F^{\mathrm{unr}}(\pi)$ is totally ramified of degree $e = \deg(q(x))$ over $F^{\mathrm{unr}}$ and $v_p(\pi) = 1/e$.

We used the branch of the logarithm for which $\log(p) = 0$ (see Remark 2.2), which, as mentioned in Remark 7.4, only makes a difference in (2) and (4), corresponding to Tables 2 and 4 respectively. The algorithm was implemented in version 2.12-19 of MAGMA [14] (but using a correct implementation of the logarithm instead of the flawed built-in version) with universal estimates as in Remark 8.1, and the calculations were performed on an Intel Pentium 4 CPU (2.66GHz) with 500MB of RAM. The programs that were used for creating Tables 1 through 4 are available on `http://www.few.vu.nl/~jeu`.

Tables 1 through 4 correspond precisely to (1) through (4) in Algorithm 7.10 so that Theorem 8.2 corresponds to Table 3. In this table we have split out the times according to what has to be done only once for each $N$, $n$ and $p$ (Time 1, for the computation of $g_n(v)$ in (3)(a)–(c)), what has to be done once for each residue disc $U_\zeta$ (Time 2, for the computation of $F_{n,\zeta}(t)$ in (3)(d)–(f)), and the evaluation of $F_{n,\zeta}(t)$ at $z - \zeta$ (Time 3, for (3)(g)), which has to be carried out for all $z$ in $U_\zeta$ unless they are close together. Similarly the times in Table 4 have been split out according to the time needed for the computation of $H_n(t)$ and some universal constants (Time 1, corresponding to (4)(a)–(c)) and the computation of $-\log^{n-1}(z)\log(1-z)/(n-1)!$ and evaluation of $H_n(t)$ at $t = z - 1$ (Time 2, corresponding to (4)(d)–(e)).

We mention that all calculations were done from scratch for each part, whereas one could easily combine the computation of $g_n(v)$ in (3)(c) with that in (4)(b) if $p \neq 2$ by increasing gsl and/or the precision in $\mathbb{Q}_p$ as necessary. Since, in practice, for larger values of $N$, most of the time in (3) and (4) is taken up by this step, this would be a substantial saving.

TABLE 1. Timings for $\mathrm{Li}_n(\pi(\zeta-1))$.

| $q(x)$ | $n$ | $p$ | $e$ | $f$ | $N$ | Time |
|---|---|---|---|---|---|---|
| $x^8-2$ | 4 | 2 | 8 | 2 | 10 | 0.020 |
| $x^8-2$ | 4 | 2 | 8 | 2 | 100 | 0.190 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 10 | 0.030 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 100 | 0.250 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 10 | 0.010 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 100 | 0.150 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 10 | 0.010 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 100 | 0.160 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 10 | 0.000 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 100 | 0.080 |

TABLE 2. Timings for $\mathrm{Li}_n((\zeta-1)/\pi)$.

| $q(x)$ | $n$ | $p$ | $e$ | $f$ | $N$ | Time |
|---|---|---|---|---|---|---|
| $x^8-2$ | 4 | 2 | 8 | 2 | 10 | 0.100 |
| $x^8-2$ | 4 | 2 | 8 | 2 | 100 | 0.500 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 10 | 0.210 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 100 | 1.540 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 10 | 0.040 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 100 | 0.750 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 10 | 0.030 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 100 | 0.690 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 10 | 0.010 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 100 | 0.180 |

TABLE 3. Timings for $\mathrm{Li}_n(\zeta+(\zeta-1)\pi)$.

| $q(x)$ | $n$ | $p$ | $e$ | $f$ | $N$ | Time 1 | Time 2 | Time 3 |
|---|---|---|---|---|---|---|---|---|
| $x^8-2$ | 4 | 2 | 8 | 2 | 10 | 0.020 | 0.060 | 0.040 |
| $x^8-2$ | 4 | 2 | 8 | 2 | 100 | 0.100 | 0.200 | 0.130 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 10 | 0.380 | 0.330 | 0.070 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 100 | 1.630 | 1.150 | 0.250 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 10 | 0.380 | 0.570 | 0.010 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 100 | 6.980 | 1.600 | 0.080 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 10 | 2.440 | 0.630 | 0.000 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 100 | 65.850 | 2.370 | 0.060 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 10 | 7.390 | 11.110 | 0.000 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 100 | 368.070 | 14.480 | 0.030 |

TABLE 4. Timings for $\mathrm{Li}_n(1+(\zeta-1)\pi)$.

| $q(x)$ | $n$ | $p$ | $e$ | $f$ | $N$ | Time 1 | Time 2 |
|---|---|---|---|---|---|---|---|
| $x^8-2$ | 4 | 2 | 8 | 2 | 10 | 0.500 | 0.080 |
| $x^8-2$ | 4 | 2 | 8 | 2 | 100 | 4.620 | 0.300 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 10 | 0.650 | 0.160 |
| $x^4-3x+3$ | 10 | 3 | 4 | 3 | 100 | 3.470 | 0.590 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 10 | 0.330 | 0.040 |
| $x^3-11x+11$ | 5 | 11 | 3 | 3 | 100 | 7.270 | 0.270 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 10 | 1.980 | 0.030 |
| $x^3-37x+37$ | 5 | 37 | 3 | 2 | 100 | 71.260 | 0.230 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 10 | 5.750 | 0.020 |
| $x^2+101$ | 3 | 101 | 2 | 2 | 100 | 363.550 | 0.080 |

*Remark* 8.5. In (5.11) (where $p=2$) we calculate the constant term of $H_n(t)$ without ever using $g_n(v)$. We can do this also for $F_{n,\zeta}(t)$ if $p$ is any prime and $\zeta$ is any root of unity of order dividing $p^f-1$, at the cost of possibly having to adjoin the $p^f$-th roots of unity to the field. Namely, by Proposition 2.10(1) we have that

$$\mathrm{Li}_n(\zeta^{p^f}) = p^{f(n-1)} \sum_{\eta^{p^f}=1} \mathrm{Li}_n(\eta\zeta),$$

and since $\zeta^{p^f}=\zeta$ this determines the constant of integration in (4.6) just as in the proof of (5.11) because all $\eta\zeta$ lie in $U_\zeta$. However, since this involves $p^f$ evaluations as in Algorithm 7.10(3)(g) in a field of degree $p^f-p^{f-1}$ over $\mathbb{Q}_p(\zeta)$, this, in general, would be less efficient than our approach, which requires only $f$ evaluations in $\mathbb{Q}_p(\zeta)$ of $g_n(v)$. Moreover, this power series is independent of $\zeta$ and $f$ so that, once computed for given $p$ and $N$, it can be used for any residue disc $U_\zeta$ with $\zeta\neq 1$ a root of unity of order relatively prime to $p$.

## REFERENCES


[1] A. A. Beilinson. Higher regulators and values of $L$-functions. *J. Sov. Math.*, 30:2036–2070, 1985. MR760999 (86h:11103)

[2] A. Besser. Syntomic regulators and $p$-adic integration I: rigid syntomic regulators. *Israel Journal of Math.*, 120:291–334, 2000. MR1809626 (2002c:14035)

[3] A. Besser. Finite and $p$-adic polylogarithms. *Compositio Math.*, 130(2):215–223, 2002. MR1883819 (2002m:11058)

[4] A. Besser, P. Buckingham, R. de Jeu, and X.-F. Roblot. On the $p$-adic Beilinson conjecture for number fields. To appear in the special volume of the Pure and Applied Mathematics Quarterly in honour of the eightieth birthday of Jean-Pierre Serre.

[5] A. Besser and R. de Jeu. The syntomic regulator for the $K$-theory of fields. *Annales Scientifiques de l'École Normale Supérieure*, 36(6):867–924, 2003. MR2032529 (2005f:11133)

[6] A. Borel. Cohomologie de $\mathrm{SL}_n$ et valeurs de fonctions zêta aux points entiers. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 4(4):613–636, 1977. Errata in vol. 7, p. 373 (1980). MR0506168 (58:22016)

[7] R. Coleman. Dilogarithms, regulators, and $p$-adic $L$-functions. *Invent. Math.*, 69:171–208, 1982. MR674400 (84a:12021)

[8] R. Coleman and J. Teitelbaum. Numerical solution of the $p$-adic hypergeometric equation. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, pages 53–62. Amer. Math. Soc., Providence, RI, 1994. MR1279601 (95d:11079)

[9] R. de Jeu. Zagier's conjecture and wedge complexes in algebraic $K$-theory. *Compositio Mathematica*, 96:197–247, 1995. MR1326712 (96h:19005)

[10] J. Fresnel and M. van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 2004. MR2014891 (2004i:14023)
[11] C. Koç and T. Acar. Montgomery multiplication in GF($2^k$). *Des. Codes Cryptogr.*, 14(1):57–69, 1998. MR1608220 (99k:11189)
[12] P. Montgomery. Modular multiplication without trial division. *Math. Comp.*, 44(170):519–521, 1985. MR777282 (86e:11121)
[13] P. Schneider. Introduction to the Beilinson Conjectures. In *Beilinson's Conjectures on Special Values of L-Functions*, pages 1–35. Academic Press, Boston, MA, 1988. MR944989 (89g:11053)
[14] The Magma group, Sydney. *Magma*. Available from `http://magma.maths.usyd.edu.au/`.
[15] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999. MR1689167 (2000j:68205)
[16] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997. MR1421575 (97h:11130)
[17] D. Zagier. Polylogarithms, Dedekind Zeta Functions and the Algebraic $K$-theory of Fields. In *Arithmetic algebraic geometry (Texel, 1989)*, pages 391–430. Birkhäuser Boston, Boston, MA, 1991. MR1085270 (92f:11161)

Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653, Be'er-Sheva 84105, Israel

Department of Mathematical Sciences, University of Durham, Science Laboratories, South Road, Durham DH1 3LE, United Kingdom

*Current address*: Faculteit Exacte Wetenschappen, Afdeling Wiskunde, Vrije Universiteit, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands